THE WARING PROBLEM FOR FINITE QUASISIMPLE GROUPS. II

ROBERT M. GURALNICK AND PHAM HUU TIEP

Abstract. Let G be a finite quasisimple group of Lie type. We show that there are regular semisimple elements $x, y \in G$, x of prime order, and $|y|$ is divisible by at most two primes, such that $x^G \cdot y^G \supseteq G \setminus Z(G)$. In fact in all but four cases, y can be chosen to be of square-free order. Using this result, we prove an effective version of one of the main results of [LST1] by showing that, given any integer $m \geq 1$, if the order of a finite simple group S is at least m^{8m^2}, then every element in S is a product of two m^{th} powers. Furthermore, the verbal width of x^m on any finite simple group S is at most $40m\sqrt{8\log_2 m} + 56$. We also show that, given any two non-trivial words w_1, w_2, if G is a finite quasisimple group of large enough order, then $w_1(G)w_2(G) \supseteq G \setminus Z(G)$.

1. Introduction

Let G be a finite non-abelian simple group, or more generally, a finite quasisimple group (that is, $G = [G, G]$ and $G/Z(G)$ is simple). Recently, various problems involving G, such as Waring-type problems and generation problems, cf. for instance [MSW], [LST1], [GM], have been resolved, crucially relying on the fact that every non-central element of G is a product of conjugates of two specific elements in G. Building on earlier work of [MSW], [LST1], and [GM], we prove the following refinement of these results on covering non-central elements in finite quasisimple groups of Lie type:

Theorem 1.1. *Let $\mathcal{G}$ be a simple simply connected algebraic group in characteristic $p > 0$ and let $F : \mathcal{G} \to \mathcal{G}$ be a Frobenius endomorphism such that $G := \mathcal{G}^F$ is quasisimple. Then there exist (not necessarily distinct) primes $r, s_1, s_2 \neq p$ and regular semisimple elements $x, y \in G$ such that $|x| = r$, y is an $\{s_1, s_2\}$-element, and $x^G \cdot y^G \supseteq G \setminus Z(G)$. In fact $s_1 = s_2$ unless $\mathcal{G}$ is of type B_{2n} or C_{2n}. Moreover, if*

$$G \notin \{SL_2(5), SL_2(17), Sp_4(3), Spin_9(3)\}$$

then the order of y can also be chosen to be square-free.

2000 *Mathematics Subject Classification.* 20D05, 20C33.

Key words and phrases. Waring problem, simple groups of Lie type.

The authors were partially supported by the NSF (grants DMS-1001962, DMS-0901241, and DMS-1201374). The first author was also partially supported by the Simons Foundation Fellowship 224965.

Corollary 1.2. *Let $\mathcal{G}$ be a simple simply connected algebraic group in positive characteristic and let $F : \mathcal{G} \to \mathcal{G}$ be a Frobenius endomorphism such that $G := \mathcal{G}^F$ is quasisimple. Assume in addition that*

$$G \notin \{SL_2(5), SL_2(17), Sp_4(3)\}.$$

Then there exist (not necessarily distinct) primes r, s_1, s_2 with the following properties:

(i) *There are elements $x, y \in G$ of square-free order such that x is regular semisimple of order r, y is an $\{s_1, s_2\}$-element, and $x^G \cdot y^G \supseteq G \setminus Z(G)$. In fact $s_1 = s_2$ unless $\mathcal{G}$ is of type B_{2n} or C_{2n}. Furthermore, y can also be chosen to be regular semisimple unless possibly $G \cong Spin_9(3)$.*

(ii) *For any elements $a, b, c \in G$ of order r, $a^G \cdot b^G \cdot c^G = G$.*

Corollary 1.3. *Let S be a finite non-abelian simple group. Then there exist (not necessarily distinct) primes r, s_1, s_2 and elements $x, y \in S$ such that*

(i) *$|x| = r$,*

(ii) *either $|y| = s_1$, or $S \in \{PSp_{4n}(q), \Omega_{4n+1}(q)\}$, $s_1 \neq s_2$ and $|y| = s_1 s_2$,*

(iii) *$x^S \cdot y^S \supseteq S \setminus \{1\}$, $x^S \cdot x^S \cdot x^S = S$.*

Moreover, if S is of Lie-type then x and y can be chosen to be regular semisimple.

Note that a (slightly weaker) version of Theorem 1.1 also holds for $r = s = p$: every non-central element of G is a product of two unipotent elements, cf. [EG, Corollary, p. 3661]. Furthermore, in a sense Corollary 1.3 yields another approximation towards Thompson's conjecture (which states that every finite non-abelian simple group S possesses a conjugacy class C such that $C^2 = S$). We also note that an asymptotic version of Corollary 1.3(iii) was established in [Sh, Corollary 2.3]: *Every large enough finite simple group S has a conjugacy class C such that $C^3 = S$.*

Theorem 1.1 allows us to prove the following effective version of the main result of [LST1] for the Waring problem in the case of powers:

Theorem 1.4. *Let $k, l \geq 1$ be any two integers and let $m := \max(k, l)$. If S is any finite simple group of order at least m^{8m^2}, then every element in S can be written as $x^k \cdot y^l$ for some $x, y \in S$.*

The main result of [LST1] implies that the *width* of the word $w(x) = x^m$ on any finite non-abelian simple group S is 2 (that is, every element of S is a product of two values of w on S), if $|S|$ is sufficiently large (but no explicit bound is given). Theorem 1.4 shows in particular that the width of $w(x) = x^m$ on any finite simple group S is 2 if $|S| \geq m^{8m^2}$.

Without *any condition* on $|S|$, Theorem 1.4 becomes false – there are various examples, cf. §3, showing that the width of x^m can grow unbounded even on simple groups S containing non-trivial m^{th} powers. However, the width of x^m on any finite simple group S is bounded universally, say by 70, see Corollary 3.9, as long as there is a prime p that divides $|S|$ but not m. More generally, we prove

Corollary 1.5. *Let $m \geq 1$ be any integer and let S be any finite simple group such that m is not divisible by $\exp(S)$. Then any element of S is a product of at most*

$$f(m) := 40m\sqrt{8\log_2 m} + 56$$

m^{th} powers in S.

Corollary 1.5 implies that, for any $m \geq 1$, the *verbal width* of the word x^m on any finite simple group S is at most $f(m)$ (i.e. any element of the subgroup $\langle g^m \mid g \in S\rangle$ is a product of at most $f(m)$ m^{th} powers in S). Thus Corollaries 1.5 and 3.9 yield effective versions of the main results of [MZ] and [SW]. For arbitrary finite groups, the verbal width of the word x^m on any d-generated finite group is bounded universally by an (implicit) function of m and d, see [NS, Theorem 1].

For an arbitrary word $w \neq 1$, the main result of [LST2] shows that the width of w on any finite quasisimple group G is at most 3 (that is, every element in G is a product of at most 3 values of w on G), if $|G|$ is sufficiently large. It remained an open question whether every *non-central* element of G is a product of at most 2 values of w on G. Our next result answers this question in the affirmative:

Theorem 1.6. (i) *Let $w \in F_d$ be a non-trivial word in the free group on d generators. Then there exists a constant $N = N_w$ depending on w such that for all finite quasisimple groups G of order greater than N we have $w(G)^2 \supseteq G \setminus Z(G)$.*

(ii) *Let $w_1, w_2 \in F_d$ be two non-trivial words in the free group on d generators. Then there exists a constant $N = N_{w_1,w_2}$ depending on w_1 and w_2 such that for all finite quasisimple groups G of order greater than N we have $w_1(G)w_2(G) \supseteq G \setminus Z(G)$.*

As shown in [LST2, Corollary 4.3], central elements are real obstructions for $w(G)^2$, respectively $w_1(G)w_2(G)$, to coincide with G. Furthermore, there are many non-trivial words w (for instance $w(x) = x^2$) which are not surjective on any finite quasisimple group. So in this sense, Theorem 1.6 is best possible for finite quasisimple groups.

The paper is organized as follows. First we prove Theorems 1.1 and Corollaries 1.2 and 1.3 in §2. In §3 we prove Theorem 1.4, Corollary 1.5 and further results on the Waring problem for powers. Finally, Theorem 1.6 is established in §4.

2. Covering non-central elements in quasisimple groups of Lie type

This section is devoted to prove Theorem 1.1 and Corollaries 1.2, 1.3. Keep the notation of the theorem. Note that if $x, y \in G$ are regular semisimple, then a result essentially proved by Gow [Gow], cf. [GT, Lemma 5.1], shows that $x^G \cdot y^G$ contains every non-central semisimple element of G. We also record the following observation:

Lemma 2.1. *In the notation of Theorem 1.1, let r be a prime with the following properties:*

(i) *Any element of order r in G is regular semisimple.*

(ii) *For any $x \in G$ of order r, there exists a regular semisimple element $y \in G$ such that $x^G \cdot y^G \supseteq G \setminus Z(G)$.*
Then $a^G \cdot b^G \cdot c^G = G$ for any elements $a, b, c \in G$ of order r.

Proof. We apply (ii) to $x = a$. As mentioned above, $y \in b^G \cdot c^G$ since b and c are both regular semisimple (and y is certainly non-central semisimple). Hence,

$$G \setminus Z(G) \subseteq a^G \cdot y^G \subseteq a^G \cdot b^G \cdot c^G.$$

On the other hand, if $z \in Z(G)$, then zc^{-1} is non-central semisimple and so $zc^{-1} \in a^G \cdot b^G$, whence $z \in a^G \cdot b^G \cdot c^G$. $\square$

In what follows, we will choose r to satisfy the condition (i) of Lemma 2.1. Hence, fixing any $x \in G$ of order r and choosing y suitably, it suffices to show that $g \in x^G \cdot y^G$, equivalently,

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x)\chi(y)\overline{\chi}(g)}{\chi(1)} > 0 \tag{1}$$

for all non-central non-semisimple elements $g \in G$.

2.1. **Type D_n with $2|n \geq 4$.** Throughout this subsection, let $\mathcal{G}^F = G = Spin^+_{2n}(q)$ with $2|n \geq 4$. In this case, it is already proved in [LST1, Theorem 1.1.4] and [GM, Theorem 7.6] that G possesses two regular semisimple elements y_1, y_2 such that $y_1^G \cdot y_2^G$ contains $G \setminus Z(G)$. But the order of one of these two elements is *not* a prime power; moreover, the pair of maximal tori containing these elements does not work well in further applications that we have in mind, including Theorems 1.4 and 1.6.

Note that Theorem 1.1 and Corollaries 1.2, 1.3 hold for $G = \Omega_8^+(2)$ by choosing x, $y \in G$ of order 7 (as one can check using [GAP]). In what follows we will therefore assume that $(n, q) \neq (4, 2)$. Following the approach of [LST1, §2], we consider some F-stable maximal tori $\mathcal{T}_1$, $\mathcal{T}_2$ of $\mathcal{G}$ such that $T_1 := \mathcal{T}_1^F$ is of type $T^{+,+}_{n-1,1}$ (so it has order $(q^{n-1}-1)(q-1)$) and $T_2 := \mathcal{T}_2^F$ is of type $T^{-,-}_{n-1,1}$ (so it has order $(q^{n-1}+1)(q+1)$).

Lemma 2.2. *Suppose $2|n \geq 4$. Then the tori T_1 and T_2 are weakly orthogonal in the sense of* [LST1, Definition 2.2.1].

Proof. We follow the proof of [LST1, Proposition 2.6.1]. Here, the dual group G^* is $PCO(V)^\circ$, where $V = \mathbb{F}_q^{2n}$ is endowed with a suitable quadratic form Q; see [TZ1, Lemma 7.4] for an explicit description of the groups G^* and $H := CO(V)^\circ$. Consider the complete inverse images in H of the tori dual to T_1 and T_2, and assume g is an element belonging to both of them. We need to show that $g \in Z(H)$. To this end, consider the spectrum S of the semisimple element g on V as a multiset. Let $\gamma \in \mathbb{F}_q^\times$ be the *conformal coefficient* of g, i.e. $Q(g(v)) = \gamma Q(v)$ for all $v \in V$. Then S can be

represented as the joins of multisets $X \sqcup Y$ and $Z \sqcup T$, where

$$X := \{x, x^q, \dots, x^{q^{n-2}}, \gamma x^{-1}, \gamma x^{-q}, \dots, \gamma x^{-q^{n-2}}\}, \quad Y := \{y, \gamma y^{-1}\},$$
$$Z := \{z, z^q, \dots, z^{q^{n-2}}, \gamma z^{-1}, \gamma z^{-q}, \dots, \gamma z^{-q^{n-2}}\}, \quad T := \{t, \gamma t^{-1}\},$$

for some $x, y, z, t \in \overline{\mathbb{F}}_q^\times$; furthermore, $x^{q^{n-1}-1} = 1 = y^{q-1}$ and $z^{q^{n-1}+1} = \gamma = t^{q+1}$.

Since $|S| = 2n < |X| + |Z| = 4n - 4$, we may assume that $x \in X \cap Z$. It follows that $x^2 = \gamma$ and so $x^{2(q-1)} = 1$. As n is even, we see that $|x|$ divides $\gcd(2(q-1), q^{n-1}-1) = q-1$, i.e. $x \in \mathbb{F}_q^\times$. Thus $X = Z = \underbrace{\{x, x, \dots, x\}}_{2n-2}$ (as multisets). In turn, this forces $Y \cap T \neq \emptyset$ and so we may assume that $y \in Y \cap T$. Arguing as with x, we get $y \in \mathbb{F}_q^\times$, $y^2 = \gamma$, and $Y = T = \{y, y\}$. Recall that $x^2 = \gamma$. Now if $x = y$, then $S = \underbrace{\{x, x, \dots, x\}}_{2n}$ and so $g \in Z(H)$ as g is semisimple.

Assume that $x \neq y$, whence q is odd and $y = -x$. Using the decomposition $S = X \sqcup Y$, we see that V is the orthogonal sum $V_1 \oplus V_2$, where $V_1 = \mathrm{Ker}(g - x \cdot 1_V)$ and $V_2 = \mathrm{Ker}(g + x \cdot 1_V)$. Moreover, since T_1 has type $T^{+,+}_{n-1,1}$, V_1 and V_2 are both of type $+$. But then the same argument applied to the decomposition $S = Z \sqcup T$ and the torus T_2 implies that V_1 and V_2 must be both of type $-$, a contradiction. $\square$

By [Zs], since $n - 1 \geq 3$ is odd, $q^{n-1} - 1$ has a *primitive prime divisor* r, i.e. r divides $q^{n-1} - 1$ but not $\prod_{i=1}^{n-2}(q^i - 1)$. In what follows, we will let $\mathrm{ppd}(q, n)$ denote any such divisor. Similarly, we take $s = \mathrm{ppd}(q, 2n-2)$ (which exists since we are assuming $(n, q) \neq (4, 2)$). Arguing as in the proof of [MT, Lemma 2.4], we can show that any element $x \in G$ of order r is regular semisimple, and certainly we can choose $x \in T_1$. Similarly, we can find a regular semisimple element $y \in T_2$ of order s. In fact, if $(n, q) \neq (4, 4)$, then, writing $q = p^f$, we can choose $r = \mathrm{ppd}(p, (n-1)f)$ and $s = \mathrm{ppd}(p, 2(n-1)f)$, which ensures that $r > (n-1)f$ and $s > 2(n-1)f$.

With the above choice of (x, y), we prove the following key statement:

Proposition 2.3. *There exist precisely four irreducible characters of G which are nonzero on both x and y: the principal character 1_G, the Steinberg character St, and two more unipotent characters α and β of degree*

$$\alpha(1) = \frac{(q^n - 1)(q^{n-1} + q)}{q^2 - 1}, \ \beta(1) = \frac{q^{n^2-3n+3}(q^n - 1)(q^{n-2} + 1)}{q^2 - 1}.$$

All of them take values ± 1 at x and at y.

Proof. 1) Consider any $\chi \in \mathrm{Irr}(G)$ with $\chi(x)\chi(y) \neq 0$. Since T_1 and T_2 are weakly orthogonal by Lemma 2.2, χ must be unipotent by [LST1, Proposition 2.2.2]. Now for $n = 4$ the statement follows by inspecting the values of the unipotent characters of G as given in Chevie [Chev]. From now on we will assume $n \geq 6$.

To identify χ among the unipotent characters of G, one could follow the proof of Propositions 3.3.1 and 7.1.1 of [LST1], but instead we will use the hook-cohook

approach of [LMT, §3.3]. Let χ correspond to the *symbol* $S = (X, Y)$ which is a pair of strictly increasing sequences $X = (x_1 < \ldots < x_k)$, $Y = (y_1 < \ldots < y_l)$ of non-negative integers, with $0 \notin X \cap Y$,

$$n = \sum_{i=1}^{k} x_i + \sum_{j=1}^{l} y_j - \frac{(k+l)(k+l-2)}{4}, \tag{2}$$

and $4|(k-l)$. (Such a symbol corresponds to two unipotent characters of G if $X = Y$.) A *hook of* S is a pair $(b, c) \in \mathbb{Z}^2$ with $0 \leq b < c$ and either $b \notin X$, $c \in X$, or $b \notin Y$, $c \in Y$. A *cohook of* S is a pair $(b, c) \in \mathbb{Z}^2$ with $0 \leq b < c$ and either $b \notin Y$, $c \in X$, or $b \notin X$, $c \in Y$. We also set

$$a(S) := \sum_{\{b,c\} \subseteq S} \min\{b, c\} - \sum_{i \geq 1} \binom{k+l-2i}{2},$$

where the first sum runs over all 2-element subsets of the multiset $X \cup Y$ of entries of S, and $b(S) = \lfloor |S-1|/2 \rfloor - |X \cap Y|$ if $X \neq Y$, respectively $b(S) = 0$ else. Then

$$\chi(1) = q^{a(S)} \frac{|G|_{q'}}{2^{b(S)} \prod_{(b,c)\text{ hook}}(q^{c-b}-1) \prod_{(b,c)\text{ cohook}}(q^{c-b}+1)}, \tag{3}$$

where the products run over hooks, respectively cohooks of S, cf. [M2, Bem. 3.12 and 6.8].

2) First we use (2) to bound x_k and y_l in terms of n. Recall that $4|t := k - l$. If $x_1 = 0$, then $y_1 \geq 1$, $y_j \geq j$, and $x_i \geq i - 1$, whence

$$n \geq x_k + \sum_{i=1}^{k-1}(i-1) + \sum_{j=1}^{l} j - \frac{(k+l)(k+l-2)}{4} = x_k + \frac{(t-2)^2}{4}. \tag{4}$$

If $x_1 \geq 1$ (including the case $k = 1$), then $x_i \geq i$, $y_j \geq j - 1$, and so

$$n \geq x_k + \sum_{i=1}^{k-1} i + \sum_{j=1}^{l}(j-1) - \frac{(k+l)(k+l-2)}{4} = x_k + \frac{t^2}{4}. \tag{5}$$

In particular, (4) and (5) imply that $x_k \leq n$ and similarly $y_l \leq n$. Without loss we may also assume that $x_k \geq y_l$.

3) Under our assumptions on (n, q), one can check that, if $1 \leq i \leq n$ and $\epsilon = \pm$, then $r|(q^i - \epsilon)$ only when $(i, \epsilon) = (n-1, +)$ and $s|(q^j - \epsilon)$ only when $(j, \epsilon) = (n-1, -)$. By 2), for any hook (b, c) we have $1 \leq c - b \leq n$. Now if $c - b \neq n - 1$ for all hooks (b, c), then (3) implies that χ has r-defect 0 and so $\chi(x) = 0$, a contradiction. So S must admit a hook $(i, n - 1 + i)$ for some $i = 0, 1$. Similarly, S possesses a cohook $(j, n - 1 + j)$ for some $j = 0, 1$. In particular, $x_k \geq n - 1$.

4) Consider the case $x_k > n-1$, whence $x_k = n$ by 2). If $x_1 = 0$, then (4) implies that $t = 2$, contradicting the condition $4|t$. So $x_1 > 0$, and so (5) (and its proof) implies that $t = 0$, $k = l$,

$$X = \{1, 2, \ldots, k-1, n\},\ Y = \{0, 1, \ldots, k-1\}.$$

Now if $k = 1$, then $S = (\{n\}, \{0\})$, yielding $\chi = 1_G$. If $k = n$, then

$$X = \{1, 2, \ldots, n\},\ Y = \{0, 1, \ldots, n-1\},$$

yielding $\chi = \mathsf{St}$. In the remaining cases, $2 \leq k \leq n-1$, and so S cannot admit any hook of the form $(i, n-1+i)$.

5) Assume now that $x_k = n-1 \geq y_l$; in particular, $(0, n-1)$ is both a hook and a cohook for S. Suppose first that $x_1 = 0$. In this case, (4) and the condition $4|t$ imply that $t = 0$ or 4,

$$X = \{0, 1, \ldots, k-2, n-1\},\ Y = \{1, 2, \ldots, l\}.$$

Also, since $0 \in X$ and $(0, n-1)$ is a hook, we have $n-1 \in Y$, implying $y_l = l = n-1$. Next, $k \leq n$ and $k - l = t \in \{0, 4\}$, so $k = n-1$,

$$X = \{0, 1, \ldots, n-4, n-3, n-1\},\ Y = \{1, 2, \ldots, n-2, n-1\},$$

leading to the character β which has the degree listed in the proposition, as one can see using (3).

Suppose now that $x_1 \geq 1$. Since $4|t$, (5) and its proof imply that $k = l$, and one of the following two cases occurs:

(a) $X = \{1, 2, \ldots, k-1, n-1\}$, $Y = \{0, 1, \ldots, k-2, k\}$, with $1 \leq k \leq n-1$, or

(b) $X = \{1, 2, \ldots, k-2, k, n-1\}$, $Y = \{0, 1, \ldots, k-1\}$, with $2 \leq k \leq n-2$.

In the case of (a), if $k = 1$ then $S = (\{n-1\}, \{1\})$ and $\chi = \alpha$. On the other hand, if $2 \leq k \leq n-1$, then $(0, n-1)$ can be a cohook for S only when $k = n-1$, leading again to $\chi = \beta$. In the case of (b), $(0, n-1)$ cannot be a cohook of S.

6) We have shown that $\chi \in \{1_G, \alpha, \beta, \mathsf{St}\}$. It remains to prove that $\chi(x), \chi(y) \in \{1, -1\}$. The statement is obvious if $\chi = 1_G$ or $\chi = \mathsf{St}$. Consider the case $\chi = \alpha$. Note that $\mathrm{Irr}(G)$ contains a unique irreducible character of degree $\alpha(1)$. (Indeed, the claim is a consequence of [TZ1, Theorem 7.6] if $q \geq 4$, and it follows from [N, Theorem 1.3] if $q < 4$.) On the other hand, it is well known (see e.g. [ST, Table 1]) that the rank 3 permutation character ρ of G (acting on the singular 1-spaces of the natural module $V = \mathbb{F}_q^{2n}$) is the sum of 1_G, an irreducible character of degree $\alpha(1)$, and another one, say γ, of degree $(q^{2n} - q^2)/(q^2 - 1)$. It follows that $\rho = 1_G + \alpha + \gamma$. Note that γ has r-defect 0 and s-defect 0. Also, it easy to see that $\rho(x) = 2$ and $\rho(y) = 0$. Hence $\alpha(x) = \rho(x) - 1 = 1$ and $\alpha(y) = \rho(y) - 1 = -1$.

7) To prove the statement in the case $\chi = \beta$, we use the Alvis-Curtis duality functor $D_{\mathcal{G}}$ which sends any irreducible character of G to an irreducible character of G up to a sign, cf. [DM, Corollary 8.15]. In the case of an F-stable torus $\mathcal{T}$, $D_{\mathcal{T}}(\lambda) = \lambda$ for

all $\lambda \in \mathrm{Irr}(\mathcal{T}^F)$, see [DM, Definition 8.8]. Applying this and [DM, Corollary 8.16] to $\mathcal{T}_1 = C_{\mathcal{G}}(x)$ (so that $T_1 = \mathcal{T}_1^F$), we now see that there is some $\epsilon_{\mathcal{G}} = \pm 1$ such that

$$\epsilon_{\mathcal{G}} D_{\mathcal{G}}(\alpha)(x) = \pm(D_{\mathcal{T}_1} \circ \mathrm{Res}^G_{T_1})(\alpha)(x) = \pm\alpha(x) = \pm 1,$$

i.e. $D_{\mathcal{G}}(\alpha)(x) = \pm 1$. Similarly, $D_{\mathcal{G}}(\alpha)(y) = \pm 1$. In particular, by the results proved above, there is some $\epsilon = \pm 1$ such that $D_{\mathcal{G}}(\alpha) = \epsilon\delta$ and $\delta \in \{1_G, \alpha, \beta, \mathsf{St}\}$.

Clearly, we are done if $\delta = \beta$. So assume that $\delta \neq \beta$. It is well known, see e.g. Corollary 8.14 and Definition 9.1 of [DM], that $D_{\mathcal{G}}$ interchanges 1_G and St. It follows that $\delta = \alpha$, i.e. $D_{\mathcal{G}}(\alpha) = \epsilon\alpha$. Now we can find an F-stable parabolic subgroup $\mathcal{P}$ with an F-stable Levi subgroup $\mathcal{L}$ such that the rank 3 permutation character ρ mentioned in 6) is just the Harish-Chandra induction $R^{\mathcal{G}}_{\mathcal{L}}(1_L)$ for $L := \mathcal{L}^F$. Applying Curtis's Theorem 8.11 of [DM], we get

$$D_{\mathcal{G}}(\rho) = D_{\mathcal{G}}(R^{\mathcal{G}}_{\mathcal{L}}(1_L)) = R^{\mathcal{G}}_{\mathcal{L}}(D_{\mathcal{L}}(1_L)) = R^{\mathcal{G}}_{\mathcal{L}}(\mathsf{St}_L),$$

where $D_{\mathcal{L}}(1_L) = \mathsf{St}_L$ is the Steinberg character of L. We will view St_L as an irreducible character σ of $P := \mathcal{P}^F$ by inflation. Also, since $D_{\mathcal{G}}$ is self-adjoint, cf. [DM, Proposition 8.10], we have

$$[D_{\mathcal{G}}(\rho), D_{\mathcal{G}}(\rho)]_G = [\rho, \rho]_G = 3.$$

It follows that $D_{\mathcal{G}}(\rho) = \mathsf{St} + \epsilon\alpha + D_{\mathcal{G}}(\gamma)$, and $D_{\mathcal{G}}(\gamma)$ is irreducible up to a sign. Furthermore, since $R^{\mathcal{G}}_{\mathcal{L}}$ is just the Harish-Chandra induction from L to G, we get

$$[\rho, D_{\mathcal{G}}(\rho)]_G = [\rho, \mathrm{Ind}^G_P(\sigma)]_G = [\mathrm{Res}^G_P(\rho), \sigma]_P = [\mathrm{Res}^G_P(1_G + \alpha + \gamma), \sigma]_P = 0$$

as α and γ have degree smaller than $\sigma(1) = |L|_p = q^{(n-1)(n-2)}$ (recall that $n \geq 6$). Note that $D_{\mathcal{G}}(\gamma) \neq \pm 1_G, \pm\alpha$ and $\rho = 1_G + \alpha + \gamma$. It follows that $D_{\mathcal{G}}(\gamma) = -\epsilon\gamma$. Hence

$$R^{\mathcal{G}}_{\mathcal{L}}(\mathsf{St}_L)(1) = [G : L]_{p'} \cdot q^{(n-1)(n-2)}$$

is equal to

$$D_{\mathcal{G}}(\rho)(1) = \mathsf{St}(1) + \epsilon(\alpha(1) - \gamma(1)) = q^{n(n-1)} + \epsilon\left(\frac{(q^n-1)(q^{n-1}+q)}{q^2-1} - \frac{q^{2n}-q^2}{q^2-1}\right),$$

yielding a contradiction, since the latter is not divisible by q^2. □

Now we can complete the case $n = 4$:

Lemma 2.4. *If $n = 4$, then $x^G \cdot y^G = G \setminus Z(G)$.*

Proof. It suffices to prove (1) for every non-semisimple $g \in G \setminus Z(G)$. For such a g, $\mathsf{St}(g) = 0$. Furthermore, inspecting the character values of α and β as given in Chevie [Chev], we see that

$$\left|\frac{\alpha(g)}{\alpha(1)}\right| + \left|\frac{\beta(g)}{\beta(1)}\right| \leq \frac{2q^3+q}{q(q^2+1)^2} + \frac{q^7}{q^7(q^2+1)^2} < 1/2,$$

and so we are done by Proposition 2.3. □

Next we estimate the character ratios $|\alpha(g)/\alpha(1)|$ for the character α described in Proposition 2.3.

Lemma 2.5. *Assume q is odd and $n \geq 6$. Then $|\alpha(g)/\alpha(1)| < 0.4$ for all $g \in G \backslash Z(G)$.*

Proof. As mentioned in p. 6) of the proof of Proposition 2.3, α is the unique irreducible character of G of degree $\alpha(1)$. Hence we may assume that α is the character $D^\circ_{1_S} = D_{1_S} - 1$ of $\bar{G} = \Omega^+_{2n}(q)$ constructed in [LBST1, §5] using the dual pair $\bar{G} * S$ inside $Sp_{4n}(q)$, with $S := Sp_2(q)$. In particular,

$$\alpha(g) = \frac{1}{|S|}\sum_{x \in S}\omega(xh) - 1$$

if $h \in \bar{G}$ corresponds to g, and ω is a *reducible Weil character* of degree q^{2n} of $Sp_{4n}(q)$. Denote

$$m(h) = \max_{\lambda \in \mathbb{F}_{q^2}} \dim \operatorname{Ker}(h - \lambda \cdot 1_V),$$

where $V = \overline{\mathbb{F}}_q^{2n}$. Since $g \notin Z(G)$, $m(h) \leq 2n - 1$.

First assume that $m(h) \leq 2n-4$. Arguing as in the proof of [LBST1, Proposition 5.11], one sees that $|\alpha(g)| \leq q^{2n-4} + 1$. On the other hand, $\alpha(g) > q^{2n-3}$. Hence

$$\left|\frac{\alpha(g)}{\alpha(1)}\right| < \frac{q^{2n-4}+1}{q^{2n-3}} < 0.4$$

as $n \geq 6$ and $q \geq 3$.

Next suppose that $m(h) \geq 2n-3$. Then h has an eigenvalue $\lambda_0 = \pm 1$ such that $\dim \operatorname{Ker}(h - \lambda_0 \cdot 1_V) = m(h)$, and $\dim \operatorname{Ker}(h - \lambda \cdot 1_V) \leq 3$ for all $\lambda \in \mathbb{F}_{q^2} \setminus \{\lambda_0\}$. Using [LBST1, Lemma 5.9] and arguing as in the proof of [LBST1, Proposition 5.11], we see that

$$|\omega(xh)| \leq \begin{cases} q^{2n-1}, & x = \begin{pmatrix} \lambda_0 & 0 \\ 0 & \lambda_0 \end{pmatrix}, \\ q^n, & x \text{ is } GL_2(q)\text{-conjugate to } \begin{pmatrix} \lambda_0 & 1 \\ 0 & \lambda_0 \end{pmatrix}, \\ q^3, & \text{otherwise} \end{cases}$$

for all $x \in S$. It follows that

$$|\alpha(g)| \leq 1 + \frac{q^{2n-1} + (q^2-1)q^n + (q(q^2-1) - q^2)q^3}{q(q^2-1)} < \frac{q^{2n-2} + q^{n+1} + q^5}{q^2-1}$$

and so

$$\left|\frac{\alpha(g)}{\alpha(1)}\right| < \frac{q^{2n-2} + q^{n+1} + q^5}{(q^n-1)(q^{n-1}+q)} < 0.4$$

as well. □

Lemma 2.6. *Assume q is even and $n \geq 6$. Then $|\alpha(g)/\alpha(1)| < 0.4$ for all $g \in G \backslash \{1\}$.*

Proof. Again consider the rank 3 permutation character $\rho = 1_G+\alpha+\gamma$ of $G = \Omega^+_{2n}(q)$. Our proof relies on the following key formula proved in [GMT]:

$$\gamma(g) = \frac{1}{2}\left(\frac{1}{q-1}\sum_{i=0}^{q-2} q^{\dim \mathrm{Ker}(g-\delta^i\cdot 1_{\tilde{V}})} - \frac{1}{q+1}\sum_{j=0}^{q}(-q)^{\dim \mathrm{Ker}(g-\xi^j\cdot 1_{\tilde{V}})}\right) - 1 \quad (6)$$

for some $\delta \in \mathbb{F}_q^\times$ of order $q-1$ and some $\xi \in \mathbb{F}_{q^2}^\times$ of order $q+1$. Here, $V = \mathbb{F}_q^{2n}$ is the natural module for G and $\tilde{V} = V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. As before, we define

$$m(g) = \max_{\lambda\in\mathbb{F}_{q^2}} \dim \mathrm{Ker}(g-\lambda\cdot 1_{\tilde{V}}).$$

Using (6), it was shown in [GMT] that $|\alpha(g)| \le q^{m(g)}$. In particular, if $m(g) \le 2n-4$, then

$$\left|\frac{\alpha(g)}{\alpha(1)}\right| \le \frac{q^{2n-4}(q^2-1)}{(q^n-1)(q^{n-1}+q)} < 0.4$$

since $n \ge 6$.

Thus we may assume that $m(g) \ge 2n-3$; in particular, $\dim \mathrm{Ker}(g-1_V) = m(g)$. But $\dim \mathrm{Ker}(g-1_V)$ is even since $g \in \Omega^+_{2n}(q)$, cf. [Atlas, p. xii]. Also, $m(g) < 2n$ as $g \ne 1$. It follows that $\dim \mathrm{Ker}(g-1_V) = 2n-2$. Now we can have the following two possibilities.

(a) The multiplicity of 1 as an eigenvalue of g (acting on V) is $2n-2$. In this case, $g = I_{2n-2}\oplus h$ for some semisimple element $1 \ne h \in Sp_2(q)$. Thus h is conjugate (over $\overline{\mathbb{F}}_q$) to $\mathrm{diag}(\lambda,\lambda^{-1})$ for some $\lambda \in \overline{\mathbb{F}}_q^\times$ with $1 \ne \lambda^q \in \{\lambda,\lambda^{-1}\}$.

(a1) Suppose that $\lambda^q = \lambda$. Then one can check that

$$\rho(g) = 2 + \frac{(q^{n-1}-1)(q^{n-2}+1)}{q-1}$$

(since $\mathrm{Ker}(g-1_V)$ is a non-degenerate subspace of dimension $2n-2$ of type $+$). On the other hand, (6) yields $\gamma(g) = (q^{2n-2}-1)/(q^2-1)$. It follows that

$$\alpha(g) = 1 + \frac{(q^{n-1}-1)(q^{n-2}+q)}{q^2-1}.$$

(a2) Assume now that $\lambda^q = \lambda^{-1}$. Then one can check that

$$\rho(g) = \frac{(q^{n-1}+1)(q^{n-2}-1)}{q-1}$$

(since $\mathrm{Ker}(g-1_V)$ is a non-degenerate subspace of dimension $2n-2$ of type $-$). On the other hand, (6) again yields that $\gamma(g) = (q^{2n-2}-1)/(q^2-1)$. It follows that

$$\alpha(g) = -1 + \frac{(q^{n-1}+1)(q^{n-2}-q)}{q^2-1}.$$

In both of these subcases, $|\alpha(g)/\alpha(1)| < 0.4$ as $n \ge 6$.

(b) The multiplicity of 1 as an eigenvalue of g (acting on V) is $\geq 2n-1$. Since this multiplicity is even, it must equal $2n$, i.e. g is unipotent. As $\dim \mathrm{Ker}(g-1_V) = 2n-2$, we see that $g = 2J_2 \oplus I_{2n-4}$, where J_2 denotes a Jordan block of size 2 with eigenvalue 1, and furthermore g acts trivially on a non-degenerate $(2n-4)$-dimensional subspace U of V. By (6) we have $\gamma(g) = (q^{2n-2} - q^2)/(q^2 - 1)$. Let Q denote the G-invariant quadratic form on V. We can now distinguish two subcases.

(b1) $U^\perp$ is decomposable as a sum of proper nonzero non-degenerate g-invariant subspaces. By [FST, Theorem 2.5], there is a unique G-conjugacy class of elements with this property. So without loss we may assume that U has type $+$ and there is a symplectic basis (e_1, f_1, e_2, f_2) of $U^\perp$ such that

$$g \ : \ e_1 \mapsto e_1, \ e_2 \mapsto e_2, \ f_1 \mapsto e_1 + f_1, \ f_2 \mapsto e_2 + f_2,$$

and

$$Q(e_1) = Q(e_2) = 1, \ Q(f_1) = Q(f_2) = 0.$$

Then $\mathrm{Ker}(g-1_V) = \langle e_1, e_2 \rangle_{\mathbb{F}_q} \oplus U$. Observe that $\langle e_1, e_2 \rangle_{\mathbb{F}_q}$ contains exactly q singular vectors and q vectors v with $Q(v) = 1$. Next, U contains exactly $(q^{n-2}-1)(q^{n-3}+1)$ nonzero singular vectors and $(q^{n-2} - 1)q^{n-3}$ vectors u with $Q(u) = 1$. It now follows by direct count that the number of g-fixed singular 1-spaces in V is

$$\rho(g) = 1 + q \cdot (q^{n-2} - 1)q^{n-3} + q \cdot \frac{(q^{n-2} - 1)(q^{n-3} + 1)}{q - 1} = \frac{q^{2n-3} - 1}{q - 1}.$$

(b2) $U^\perp$ is indecomposable as a sum of proper nonzero non-degenerate g-invariant subspaces. By [FST, Theorem 2.5], there is a unique G-conjugacy class of elements with this property. So without loss we may assume that U has type $+$ and there is a symplectic basis (e_1, f_1, e_2, f_2) of $U^\perp$ such that

$$g \ : \ e_1 \mapsto e_1, \ e_2 \mapsto e_1 + e_2, \ f_1 \mapsto f_1 + f_2, \ f_2 \mapsto f_2$$

(so that $g|_{U^\perp}$ is a short-root element of $Sp(U^\perp)$), and

$$Q(e_1) = Q(e_2) = Q(f_1) = Q(f_2) = 0.$$

Then $\mathrm{Ker}(g - 1_V) = \langle e_1, f_2 \rangle_{\mathbb{F}_q} \oplus U$. Now $\langle e_1, f_2 \rangle_{\mathbb{F}_q}$ is totally singular, and, as before, U contains exactly $(q^{n-2} - 1)(q^{n-3} + 1)$ nonzero singular vectors. It now follows by direct count that the number of g-fixed singular 1-spaces in V is

$$\rho(g) = (q + 1) + q^2 \cdot \frac{(q^{n-2} - 1)(q^{n-3} + 1)}{q - 1} = \frac{q^{2n-3} + q^n - q^{n-1} - 1}{q - 1}.$$

In both of these subcases,

$$|\alpha(g)| = |\rho(g) - 1 - \gamma(g)| \leq \frac{q^{2n-3} + q^{n+1} - q^{n-1} - q}{q^2 - 1}.$$

It follows that $|\alpha(g)/\alpha(1)| < 0.4$ as well. $\square$

The main result of this subsection is the following

Theorem 2.7. *Let $G = Spin^+_{2n}(q)$ with $2|n \geq 4$, $(n,q) \neq (4,2)$, and let $x_1 \in T_1$ and $x_2 \in T_2$ be regular semisimple elements, where the tori T_1 and T_2 are described at the beginning of §2.1. Then $x_1^G \cdot x_2^G = G \setminus Z(G)$. In particular, $x^G \cdot y^G = G \setminus Z(G)$, where x and y are regular semisimple of order r and s.*

Proof. Note that it suffices to prove the statement for x and y. Indeed, the tori T_1 and T_2 are weakly orthogonal by Lemma 2.2. Hence, by [LST1, Proposition 2.2.2], all irreducible characters χ of G that vanish neither on a regular semisimple element $x_1 \in T_1$ nor on a regular semisimple element $x_2 \in T_2$ must be unipotent. But then the results of [DL] imply that $\chi(x_1)$ does not depend on the particular choice of $x_1 \in T_1$ of given type, and similarly for $\chi(x_2)$; in particular, $\chi(x_1) = \chi(x)$ and $\chi(x_2) = \chi(y)$. Hence, for any $g \in G$ we have

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x_1)\chi(x_2)\overline{\chi}(g)}{\chi(1)} = \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x)\chi(y)\overline{\chi}(g)}{\chi(1)}.$$

Consequently, $x_1^G \cdot x_2^G = x^G \cdot y^G$.

It remains to prove (1) for every non-semisimple $g \in G \setminus Z(G)$. Applying Lemma 2.4 we may assume that $n \geq 6$. Also, $\mathsf{St}(g) = 0$ for any such a g. Next,

$$\left|\frac{\alpha(g)}{\alpha(1)}\right| < 0.4$$

by Lemmas 2.5 and 2.6. As in the proof of [LST1, Theorem 1.1.4], we have that

$$|\beta(g)|^2 \leq |C_G(g)| \leq |G|/q^{2n-2} < q^{2n^2-3n+2}.$$

On the other hand, $\beta(1) > q^{n^2-n-1}$. It follows that

$$\left|\frac{\beta(g)}{\beta(1)}\right| < q^{2-n/2} \leq q^{-1} \leq 0.5.$$

Thus

$$\left|\frac{\alpha(g)}{\alpha(1)}\right| + \left|\frac{\beta(g)}{\beta(1)}\right| + \left|\frac{\mathsf{St}(g)}{\mathsf{St}(1)}\right| \leq 0.9,$$

and so we are done by Proposition 2.3. □

2.2. **Other Lie-type groups.** By Theorem 2.7 (and the remark at the beginning of §2.1), Theorem 1.1 and Corollaries 1.2, 1.3 hold for $G = Spin^+_{4n}(q)$. Now we will prove Theorem 1.1 and Corollaries 1.2, 1.3 for the remaining types. We will write $q = p^f$ as usual. In the cases where s_1 and s_2 can be chosen to be equal, we write $s = s_1 = s_2$.

First we deal with a few special cases.

Lemma 2.8. *Theorem 1.1 and Corollaries 1.2, 1.3 hold for $G = SL_2(q)$ with $q \geq 4$.*

Proof. Suppose first that $q \pm 1$ are not 2-powers. Then we can choose odd prime divisors r of $q-1$ and s of $q+1$, and find regular semisimple elements $x \in G$ of order r and $y \in G$ of order s. (In fact, we can choose $r = \mathrm{ppd}(p, 2f)$ and $s = \mathrm{ppd}(p, f)$ if $f \geq 7$.) Using the character table of G (see e.g. [Do, §38]), one can check that $x^G \cdot y^G = G \setminus Z(G)$.

Suppose $q-1$ is a 2-power. If $q = 9$, we can take x, y to be non-conjugate elements of order 5 in G. Otherwise q is a Fermat prime. If $q = 5$ or 17, we can choose $|x| = 3$ and $|y| = 4$ (but note that there is no desired pair (x, y) of square-free orders). For $S = PSL_2(q)$ with $q = 5$ or 17, we have $S = x^S \cdot x^S$ where $|x| = 3$. On the other hand, if $q > 17$ is a Fermat prime, then it is not difficult to show that $q + 1$ has a prime divisor $r \geq 5$. Choosing $x \in G$ of order r and using the character table of G, we can check that $x^G \cdot (x^2)^G = G \setminus Z(G)$.

Suppose now that $q + 1$ is a 2-power, i.e. $q = 2^t - 1 \geq 7$ is a Mersenne prime. Choosing $x \in G$ of order $r = t$, one can check that $x^G \cdot x^G = G \setminus Z(G)$. □

Lemma 2.9. *Theorem 1.1 and Corollaries 1.2, 1.3 hold for $G = SL_3(q)$.*

Proof. Let $r = \mathrm{ppd}(p, 3f)$ if $q \neq 2, 4$, $r = 7$ if $q = 4$, and $r = 3$ if $q = 2$. Then we can find a regular semisimple element $x \in G$ of order r. By [Gow], $x^G \cdot x^G$ contains all non-central semisimple elements of G. Direct computation using [Chev] shows that $x^G \cdot x^G$ also contains all other non-central classes of G. □

Lemma 2.10. *Theorem 1.1 and Corollaries 1.2, 1.3 hold for $G = SU_3(q)$ with $q > 2$.*

Proof. Note that $r = \mathrm{ppd}(p, 6f)$ exists since $q > 2$. Then we can find a regular semisimple element $x \in G$ of order r. Again, using [Chev] one can check that $x^G \cdot x^G \supseteq G \setminus Z(G)$. □

Lemma 2.11. *Theorem 1.1 and Corollaries 1.2, 1.3 hold for $G = Sp_4(q)$ where $q \geq 5$ is odd.*

Proof. We will follow the proof of Lemma 2.8 and use the notation and the character table of G as described in [Sri]. First we let $r = \mathrm{ppd}(p, 4f)$ and consider $x \in G$ belonging to the class $B_1((q^2+1)/r)$ (so that x is regular semisimple of order r). If both $q \pm 1$ are not 2-powers, then we can find odd primes $s_1 = \mathrm{ppd}(p, 2f)$ and $s_2 = \mathrm{ppd}(p, f)$ and consider $y \in B_2((q^2-1)/s_1 s_2)$ of order $s_1 s_2$. If $q = 9$, take $y \in B_4(2, 4)$ of order 5. If $q \geq 5$ is a Fermat prime, consider the element $y \in B_4((q+1)/6, (q+1)/3)$ of order 6. If $q \geq 7$ is a Mersenne prime, take $y \in B_3((q-1)/6, (q-1)/3)$ of order 6. In all cases, one can check that y is also regular semisimple, and $x^G \cdot y^G \supseteq G \setminus Z(G)$. □

Lemma 2.12. *Theorem 1.1 and Corollaries 1.2, 1.3 hold if G is one of the following groups:*

$$\begin{cases} SU_4(2),\ SL_6(2),\ SL_7(2),\ Sp_6(2),\ \Omega_8^-(2), \\ G_2(4),\ {}^2F_4(2)',\ Sp_4(3),\ Sp_8(3),\ Spin_9(3). \end{cases}$$

Proof. 1) Using [GAP], we can find a regular semisimple elements $x \in G = SU_4(2)$ of order 5 such that $x^G \cdot x^G \supseteq G \setminus \{1\}$. Similarly, if $G = SL_6(2)$, respectively $SL_7(2)$, $Sp_6(2)$, $\Omega_8^-(2)$, $G_2(4)$, ${}^2F_4(2)'$, we can choose $x = y$ of order 31, 127, 7, 7, 7, and 13, respectively.

The case $G = Sp_4(3)$ is a genuine exception to the main claims in Theorem 1.1 and Corollary 1.2. Using [GAP] one can check that

(i) there is no pair $(x, y) \in G \times G$ such that $x^G \cdot y^G \supseteq G \setminus Z(G)$ and $|x|$, $|y|$ are square-free;

(ii) even though $\bar{x}^S \cdot \bar{y}^S \supseteq S \setminus \{1\}$ with $|\bar{x}| = |\bar{y}| = 5$ in $S = G/Z(G)$, the pair $(\bar{x}, \bar{y})$ does not lift to any pair $(x, y) \in G \times G$ with $x^G \cdot y^G \supseteq G \setminus Z(G)$;

(iii) however, $x^G \cdot y^G = G \setminus Z(G)$ and $y^G \cdot y^G = G$ if $|x| = 5$ and $|y| = 8$.

3) Let $G = Sp_8(3)$ and consider a regular semisimple element $x \in G$ of order 41. Next, let $v \in Sp_4(3)$ be of order 10 and let

$$y := \mathrm{diag}(v, v^2) \in Sp_4(3) \times Sp_4(3) \hookrightarrow G.$$

Then y is also regular semisimple, of order 10 both in G and in $S = G/Z(G) = PSp_8(3)$. Moreover, if z denotes the central involution of G, then y and yz are conjugate in G. It follows that all faithful irreducible characters of G vanish on y. The character table of S (not of G!) is available in [GAP]. One can now check that y belongs to the class $10c$ in S, and there are precisely three irreducible characters of S which are nonzero at both x and y: 1_S, St, and α of degree $235,872$. Moreover,

$$\mathsf{St}(x) = -1,\ \mathsf{St}(y) = 1,\ \max_{g \in G \setminus Z(G)} |\mathsf{St}(g)| = 3^{10}$$

and

$$\alpha(x) = -1,\ \alpha(y) = 2,\ \max_{g \in G \setminus Z(G)} |\alpha(g)| = 29,484.$$

Thus for any $g \in G \setminus Z(G)$ we have

$$\left| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x)\chi(y)\overline{\chi}(g)}{\chi(1)} \right| \geq 1 - \frac{2 \cdot 29,484}{235,872} - \frac{3^{10}}{3^{16}} > 0.7,$$

i.e. $x^G \cdot y^G = G \setminus Z(G)$.

4) Let $G = Spin_9(3)$ and consider a regular semisimple element $x \in G$ of order 41. We can also find $y \in G$ of order 39 both in G and in $S = G/Z(G) = \Omega_9(3)$. Furthermore, there is $y' \in G$ which has order 26 in S, and y' is regular semisimple. Clearly, if $\chi \in \mathrm{Irr}(G)$ and $\chi(x)\chi(y) \neq 0$ or $\chi(x)\chi(y') \neq 0$, then $\chi(1)$ is coprime to $13 \cdot 41$. The character table of G is still unknown, but the degrees of irreducible characters of G have been determined by F. Lübeck [Lu]. Now we can check that there are precisely four irreducible characters of G of degree coprime to $13 \cdot 41$: 1_G, α of degree $1,680$, β of degree $11,022,480$, and St. The character table of S is available in [GAP], and S also has irreducible characters of these four degrees. Thus

the four aforementioned irreducible characters are actually trivial at $Z(G)$. Again using [GAP] one can check that

$$\alpha(y) = \mathsf{St}(y) = 0,\ \alpha(x) = \beta(x) = -1,\ \beta(y) = 1,\ \max_{g \in G \setminus Z(G)} |\beta(g)| = 408,240,$$

and

$$|\alpha(y')| = |\beta(y')| = |\mathsf{St}(y')| = 1,\ \max_{g \in G \setminus Z(G)} |\alpha(g)| = 560,\ \max_{g \in G \setminus Z(G)} |\mathsf{St}(g)| = 3^{12}.$$

Thus for any $g \in G \setminus Z(G)$ we have

$$\left| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x)\chi(y)\overline{\chi}(g)}{\chi(1)} \right| \geq 1 - \frac{408,240}{11,022,480} > 0,$$

i.e. $x^G \cdot y^G = G \setminus Z(G)$. Similarly,

$$\left| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x)\chi(y')\overline{\chi}(g)}{\chi(1)} \right| \geq 1 - \frac{560}{1,680} - \frac{408,240}{11,022,480} - \frac{3^{12}}{3^{16}} > 0.5$$

for all non-central $g \in G$, whence $x^G \cdot (y')^G = G \setminus Z(G)$. Furthermore, using [GAP] one can check that $x^S \cdot x^S = S$. Thus we can use the pair (x, y') for Theorem 1.1 and Corollary 1.3, and the pair (x, y) for Corollary 1.2. $\square$

In what follows we will assume that G is not isomorphic to any of the groups listed in Lemmas 2.9–2.12.

2.2.1. *Type A_m with $n \geq 3$.* Let $G = SL_n(q)$ with $n \geq 4$, $(n, q) \neq (6, 2)$, $(7, 2)$. We aim to find x and y contained in tori T_1 of order $(q^n - 1)/(q - 1)$ and T_2 of order $q^{n-1} - 1$. To this end, choose $r = \mathrm{ppd}(p, nf)$, and $s = \mathrm{ppd}(p, (n-1)f)$ if $(n, q) \neq (4, 4)$ and $s = 7$ otherwise. In all cases, it is easy to check that there exist regular semisimple elements $x \in T_1$ of order r and $y \in T_2$ of order s. In fact, any element of order r in G is regular semisimple (and the same holds in all subsequent cases of our proof). Now the tori T_1 and T_2 are weakly orthogonal (cf. [MSW, Proposition 2.1] or [LST1, Proposition 2.3.1]). Hence, by [LST1, Proposition 2.2.2], if $\chi \in \mathrm{Irr}(G)$ is nonzero at both x and y then χ is unipotent. This in turn implies by [DL] that the value of χ at any regular semisimple element in T_i does not depend on the particular choice of the element. Hence we can apply [MSW, Theorem 2.1] to conclude that $x^G \cdot y^G \supseteq G \setminus Z(G)$. (In subsequent cases we will frequently allude to this argument without mentioning it explicitly.)

2.2.2. *Type ^2A_m with $m \geq 3$.* Let $G = SU_n(q)$ with $n \geq 4$ and $(n,q) \neq (4,2)$. First we consider the case $n \geq 5$ is odd. Then we can choose $r = \mathrm{ppd}(p, 2nf)$ and find a regular semisimple element $x \in G$ of order r that belongs to a maximal torus T_1 of order $(q^n+1)/(q+1)$. Next, if $n \equiv 1 (\mathrm{mod}\, 4)$ then we choose $s = \mathrm{ppd}(p,(n-1)f)$. When $n \equiv 3 (\mathrm{mod}\, 4)$, we choose $s = \mathrm{ppd}(p,(n-1)f/2)$ if $(n,q) \neq (7,2^2)$, and $s = 7$ otherwise. One can show that there is a regular semisimple element $y \in G$ of order s that belongs to a maximal torus T_2 of order $q^{n-1}-1$. By [MSW, Theorem 2.2] we have $x^G \cdot y^G \supseteq G \setminus Z(G)$.

Suppose now that $n \geq 4$ is even. Then we can find a regular semisimple element x of order r that belongs to a maximal torus T_1 of order $q^{n-1}+1$, where $r = \mathrm{ppd}(p, 2(n-1)f)$. Next, if $n \equiv 0 (\mathrm{mod}\, 4)$ then we choose $s = \mathrm{ppd}(p, nf)$. When $n \equiv 2 (\mathrm{mod}\, 4)$, we choose $s = \mathrm{ppd}(p, nf/2)$ if $(n,q) \neq (6,2^2)$, and $s = 7$ otherwise. One can show that there is a regular semisimple element $y \in G$ of order s that belongs to a maximal torus T_2 of order $(q^n-1)/(q+1)$. Applying [MSW, Theorem 2.2] we see that $x^G \cdot y^G \supseteq G \setminus Z(G)$.

2.2.3. *Types B_n and C_n with $n \geq 2$.* Suppose that $G = Spin_{2n+1}(q)$ or $Sp_{2n}(q)$, with $n \geq 2$, $(n,q) \neq (2,2)$, $(2,3)$, $(3,2)$, $(4,3)$. We aim to find x and y contained in tori T_1 of order q^n+1 and T_2 of order q^n-1. To this end, we take $r = \mathrm{ppd}(p,2nf)$. If n is *odd*, then we choose $s = \mathrm{ppd}(p,nf)$ if $(n,q) \neq (3,4)$ and $s = 7$ if $(n,q) = (3,4)$. It is easy to check that there exist regular semisimple elements $x \in T_1$ of order r and $y \in T_2$ of order s, and furthermore $x^G \cdot y^G \supseteq G \setminus Z(G)$ by [MSW, Theorem 2.3].

Assume that $2|n$ and $n \geq 4$. Then we choose $s_1 = \mathrm{ppd}(p,nf)$ if $(n,q) \neq (6,2)$ and $s_1 = 3$ if $(n,q) = (6,2)$. Furthermore, if $n \geq 6$, we take $s_2 = \mathrm{ppd}(p,nf/2)$ when $(n,q) \neq (12,2)$ and $s_2 = 7$ when $(n,q) = (12,2)$. If $n = 4$, we choose $s_2 = \mathrm{ppd}(p,nf/2)$ whenever q is not a Mersenne prime, and $s_2 = 3$ if $q \geq 7$ is a Mersenne prime. In all cases, one can check that there exist regular semisimple elements $x \in T_1$ of order r and $y \in T_2$ of order s_1s_2. (For instance, we can choose y of order 91 if $(n,q) = (12,2)$. If $n = 4$ and $q = 2^a - 1 \geq 7$ is a Mersenne prime, then note that $Sp_8(q)$, respectively $\Omega_9(q)$, contains a cyclic subgroup of order q^4-1, respectively $(q^4-1)/2$. It follows in this case that G contains a semisimple element y of order s_1s_2, and it is easy to check that y is regular.) Now, $x^G \cdot y^G \supseteq G \setminus Z(G)$ by [MSW, Theorem 2.3].

Finally, assume that $n = 2$ and $q \geq 4$. Since $Spin_5(q) \cong Sp_4(q)$ and by Lemma 2.11, we may assume that $G = Sp_4(q)$ and $q = 2^f$. Choose $s_1 = \mathrm{ppd}(2,2f)$ if $f \neq 3$ and $s_1 = 3$ if $f = 3$, and $s_2 = \mathrm{ppd}(2,f)$ if $f \neq 6$ and $s_2 = 3$ if $f = 6$. One readily checks that there exist regular semisimple elements $x \in T_1$ of order r and $y \in T_2$ of order s_1s_2, and we are done as before. (Note that the non-simple group $Sp_4(2)$ is excluded in the above analysis; for $Sp_4(2)' \cong \mathsf{A}_6$ we can choose $r = s = 5$.)

2.2.4. *Types D_n and ^2D_n.* Note that the case of D_n with $2|n$ is already completed by Theorem 2.7. Assume now that $G = Spin^+_{2n}(q)$, where $n \geq 5$ is *odd*. Then we

can choose $r = \mathrm{ppd}(p, nf)$ and find a regular semisimple element x of order r that belongs to a maximal torus T_1 of order $q^n - 1$, see e.g. [MT, Lemma 2.4]. Similarly, we can find a regular semisimple element y of order s that belongs to a maximal torus T_2 of order $(q^{n-1}+1)(q+1)$, for some $s = \mathrm{ppd}(p, 2(n-1)f)$. By [MSW, Theorem 2.6] we have $x^G \cdot y^G \supseteq G \setminus Z(G)$.

Suppose now that $G = Spin^-_{2n}(q)$ with $n \geq 4$ and $(n, q) \neq (4, 2)$. Then we can choose $r = \mathrm{ppd}(p, 2nf)$ and find a regular semisimple element x of order r that belongs to a maximal torus T_1 of order $q^n + 1$, see e.g. [MT, Lemma 2.4]. Similarly, we can find a regular semisimple element y of order s that belongs to a maximal torus T_2 of order $(q^{n-1}+1)(q-1)$, where $s = \mathrm{ppd}(p, 2(n-1)f)$. Applying [MSW, Theorem 2.5], we conclude that $x^G \cdot y^G \supseteq G \setminus Z(G)$.

2.2.5. *Exceptional groups.* In the cases where $G = {}^2B_2(q)$ with $q \geq 8$, respectively $G = {}^2G_2(q)$ with $q \geq 27$, by [GM, Theorem 7.1] we can take $r = s = \mathrm{ppd}(2, 4f)$, respectively $r = s = \mathrm{ppd}(3, 6f)$. Similarly, in the cases where $G = G_2(q)$ with $q \neq 2$, respectively $G = {}^3D_4(q)$, by [GM, Theorem 7.2] we can take $r = s = \mathrm{ppd}(p, 3f)$ if $q \neq 4$ and $r = s = 7$ if $q = 4$, respectively $r = s = \mathrm{ppd}(p, 12f)$ (here, the existence of regular semisimple elements of order r follows from [MT, Lemma 2.3]). If $G = F_4(q)$, then G contains regular semisimple elements $x \in G$ of order $r = \mathrm{ppd}(p, 12f)$ and $y \in S$ of order $s = \mathrm{ppd}(p, 8f)$ by [MT, Lemma 2.3], and $x^G \cdot y^G = G \setminus \{1\}$ by [GM, Theorem 7.6]. Similarly, if $G = E_8(q)$, then G contains regular semisimple elements $x \in G$ of order $r = \mathrm{ppd}(p, 24f)$ and $y \in G$ of order $s = \mathrm{ppd}(p, 20f)$, and $x^G \cdot y^G = G \setminus \{1\}$ by [GM, Theorem 7.6].

Suppose that $G = E_7(q)_{sc}$. By [MT, Lemma 2.3], G contains a regular semisimple element $x \in G$ of order $r = \mathrm{ppd}(p, 18f)$ (and with centralizer of order $(q+1)(q^6 - q^3 + 1)$). Furthermore, it is shown in the proof of [HSTZ, Theorem 4.2] that there is a regular semisimple $y \in G$ of order $s = \mathrm{ppd}(p, 7f)$. Now we can apply [GM, Theorem 7.6] to conclude that $x^G \cdot y^G = G \setminus Z(G)$.

Next let $G = \mathcal{G}^F = E_6^\epsilon(q)_{sc}$, with $\epsilon = +$ for $E_6(q)_{sc}$ and $\epsilon = -$ for ${}^2E_6(q)_{sc}$. By [MT, Lemma 2.3], G contains a regular semisimple element $x \in G$ of order r, with $r = \mathrm{ppd}(p, 9f)$ if $\epsilon = +$ and $r = \mathrm{ppd}(p, 18f)$ if $\epsilon = -$ (and with centralizer of order $q^6 + \epsilon q^3 + 1$). Next we choose $s = \mathrm{ppd}(p, 8f)$ and let $y \in G$ be of order s. Applying [MT, Lemma 2.2], we see that $C_\mathcal{G}(y)$ is connected and s divides $|(Z(C_\mathcal{G}(y))^\circ)^F|$. The order of the latter (for all y) is listed in [Der]. Using this, one can easily check that $C_\mathcal{G}(y)$ is a torus, i.e. y is regular, and $|C_G(y)| = (q^4+1)(q^2-1)$. It then again follows by [GM, Theorem 7.6] that $x^G \cdot y^G = G \setminus Z(G)$.

Finally, the case of ${}^2F_4(q)$ with $q > 2$ follows from the following statement:

Lemma 2.13. *Let $G = {}^2F_4(q)'$ with $q = 2^f > 2$. Then G admits regular semisimple elements x of order $r = \mathrm{ppd}(2, 12f)$ and y of order $s = \mathrm{ppd}(2, 6f)$, such that $x^G \cdot y^G = G \setminus \{1\}$.*

Proof. The existence of regular semisimple elements $x \in G$ of order r and y of order $s \in G$ is proved in [MT, Lemma 2.3]. In particular, $|C_G(x)| = (q^2+q+1)+\epsilon\sqrt{2q}(q+1)$ for some $\epsilon = \pm$; moreover, in the notation of [M1], x is of type t_{17} if $\epsilon = +$ and of type t_{16} if $\epsilon = -$, whereas y is of type t_{15}. Suppose now that $\chi \in \mathrm{Irr}(G)$ is nonzero at both x and y, and χ belongs to the Lusztig series $\mathcal{E}(G,(t))$ labeled by the semisimple element $t \in G^* \cong G$. Since $\chi(x) \neq 0$, χ cannot have r-defect zero, and so $|C_G(t)|$ is divisible by r. Similarly, $|C_G(t)|$ is divisible by s. These condition imply that $t = 1$, i.e. χ is unipotent. The values of unipotent characters of G are determined in [M1]. An inspection of these values reveals that there are precisely four possibilities for χ: 1_G, St, and two more characters of degree $q^2(q^4-1)^2/3$, labeled by χ_{19} and χ_{20} in [M1]. Moreover,

$$\chi_{19}(x) = \chi_{20}(x) = 1,\ \chi_{19}(y) = \chi_{20}(y) = -1.$$

Now let $g \in G$ be any non-trivial element. As mentioned above, $g \in x^G \cdot y^G$ if g is semisimple. If g is not semisimple, then using [M1] we see that

$$\left|\sum_{1_G \neq \chi \in \mathrm{Irr}(G)} \frac{\chi(x)\chi(y)\overline{\chi}(g)}{\chi(1)}\right| = \left|\frac{\chi_{19}(g)+\chi_{20}(g)}{\chi_{19}(1)}\right| \leq \frac{2q^2(q^4-1)/3}{q^2(q^4-1)^2/3} = \frac{2}{q^4-1} < 0.1,$$

whence (1) holds, and so we are done. □

We have completed the proof of Theorem 1.1 and Corollary 1.2.

2.3. **Proof of Corollary 1.3.** In view of previous results, it remains to prove Corollary 1.3 for alternating and sporadic simple groups. For these groups, the statement follows from

Lemma 2.14. *Let S be an alternating or sporadic finite simple group. Then there is an element $x \in S$ of prime order r such that*

$$x^S \cdot (x^{-1})^S = x^S \cdot x^S \cdot x^S = S.$$

Moreover, if S is sporadic, then r can be chosen to be the largest prime divisor of $|S|$.

Proof. Note that if $x^S \cdot (x^{-1})^S = S$, and x is real or $x^{-1} \in x^S \cdot x^S$, then

$$S = x^S \cdot (x^{-1})^S \subseteq x^S \cdot x^S \cdot x^S.$$

Assume that $S = \mathsf{A}_n$ with $n \geq 5$. By the main result of [B], every $g \in S$ is a product of two r-cycles if $r \geq \lfloor 3n/4 \rfloor$, Moreover, if $r \leq n-2$ then the r-cycles form a unique A_n-class and they are all real. Hence we are done if the interval $[\lfloor 3n/4 \rfloor, n-2]$ contains a prime. The latter claim holds for $n \geq 33$, since then $(5(n-2)/6, n-2)$ contains a prime. It also holds for $n \geq 5$ but $n \neq 6, 8, 11, 12$ by direct inspection. In the cases $n = 6, 8, 11, 12$, a direct computation using [GAP] shows that

$$x^S \cdot (x^{-1})^S = S,\ x^{-1} \in x^S \cdot x^S \tag{7}$$

if we can choose x of order 5, 7, 11, and 11, respectively.

If S is a sporadic group and $x \in S$ is an element of largest prime order, then (7) can be verified directly using [GAP]. $\square$

3. The Waring problem for powers

3.1. **Proof of Theorem 1.4.** Note that the statement is obvious if k and l are coprime. So we will assume that $\gcd(k,l) > 1$. Now if $m \leq 5$, then the latter condition implies that m is also equal to $\mathrm{lcm}(k,l)$ and that m is a prime power. In this case, the statement follows from [GM, Corollary 1.5], which says that every element in any finite non-abelian simple group is a product of two m^{th}-powers, provided that m is a prime power.

From now we will assume that $m \geq 6$. In particular, $m^{8m^2} > 10^{223}$, and so we can ignore all the sporadic simple groups. Suppose that $S \cong \mathsf{A}_n$; in particular, $n > \max(4m, 200)$. Under this assumption, we can find a prime p such that $5n/6 < p < n$ (see e.g. [R]); in particular, $p > m$. By the main result of [B], every $g \in \mathsf{A}_n$ is a product of two p-cycles, whence it is a product of a k^{th}-power and an l^{th}-power.

Thus we may now assume that S is a simple group of Lie type of order $> 10^{223}$ and view $S = G/Z(G)$, where $G = \mathcal{G}(\mathbb{F}_q) = \mathcal{G}^F$ as in Theorem 1.1 and $q = p^f$. It suffices to show that every element $g \in G \setminus Z(G)$ is a product of two elements of orders coprime to both k and l in G. If the characteristic p of G is larger than m, then the statement follows from [EG, Corollary, p. 3661]. So we may assume that $p \leq m$. Let d denote the rank of the algebraic group $\mathcal{G}$. By Theorem 1.1 and its proof, there exist primes r, s_1, s_2 such that $g = xy$ for some r-element $x \in G$ and $\{s_1, s_2\}$-element $y \in G$; moreover, $t > df/2$ if G is classical and $t > df$ if G is exceptional for $t := \min(r, s_1, s_2)$. Certainly, we are done if $t > m$. Suppose that $t \leq m$. If G is classical, then $df \leq 2t - 1 \leq 2m - 1$, and

$$|S| < q^{d(2d+1)} \leq p^{df(2df+1)} < m^{(2m-1)(4m-1)} < m^{8m^2}.$$

If G is exceptional, then $df < t \leq m$, and

$$|S| < q^{31d} \leq p^{31df} < m^{31m} < m^{8m^2}$$

(since $m \geq 6$), completing the proof of Theorem 1.4.

The above proof of Theorem 1.4 also yields the following statement:

Corollary 3.1. (i) *Let S be a finite non-abelian simple group. Then there exist primes r, s_1, s_2 such that every non-trivial element $g \in S$ is a product of an r-element $x \in S$ and an $\{s_1, s_2\}$-element $y \in S$. Moreover, the primes r, s_1, and s_2 can be chosen to be arbitrarily large if $|S|$ is large enough.*

(ii) *Let $\mathcal{G}$ be a simple simply connected algebraic group in positive characteristic and let $F : \mathcal{G} \to \mathcal{G}$ be a Frobenius endomorphism such that $G := \mathcal{G}^F$ is quasisimple. Then there exist primes r, s_1, s_2 such that every non-central element $g \in G$ is a*

product of an r-element $x \in G$ and an $\{s_1, s_2\}$-element $y \in G$. Moreover, the primes r, s_1, and s_2 can be chosen to be arbitrarily large if $|G|$ is large enough.

3.2. **Further results on the width.** Recall that the main result of [LST1] establishes *width* 2 for arbitrary non-trivial word maps on *sufficiently large* finite simple groups S. What happens if one removes the condition on the order of S?

It has been shown in [KN] that the width can grow unbounded even when $w(S) \neq \{1\}$; namely, given any N, there is a word w in the free group on two generators and a finite simple group S such that $w(S) \neq \{1\}$ but yet $w(S)^N \neq S$.

The next two examples show that the same is true for powers.

Example 3.2. Let p be any prime, and let $S = PSL_{p^a+1}(p^b)$ for some integers $a, b \geq 1$. Set $w(x) = x^k$ with $k := \exp(S)/p$. We claim that $w(S)$ *consists of the identity and all transvections in S, and, consequently,* $w(S)^{p^a} \neq S$. Indeed, note that the p-part k_p of k is p^a. Considering the Jordan decomposition $g = su$ for any $g \in S$, we see that $g^k = (su)^k = u^k$ is non-trivial precisely when u is a Jordan block of size $p^a + 1$, in which case $g^k = u^k$ is a transvection. Now if $h = g_1 g_2 \ldots g_{p^a}$ and $g_i \in w(S)$, then, after lifting g_i to a p-element $\hat{g}_i \in G = SL_{p^a+1}(p^b) = SL(V)$, we have that codim $C_V(\hat{g}_i) \leq 1$. It follows that codim $C_V(\hat{h}) \leq p^a$, i.e. $C_V(\hat{h}) \neq 0$ for $\hat{h} := \prod_{i=1}^{p^a} \hat{g}_i$. Hence $w(S)^{p^a} \neq S$.

Of course similar examples hold for other classical groups (in characteristic p). We offer an example in cross characteristic as well:

Example 3.3. Let p be any prime, $a \geq 1$, and let $S = PSL_{p^a+1}(q)$ for some prime power q such that $p|(q-1)$. For simplicity, assume in addition that $p > 2$ and $(q-1)_p = p$. Again set $w(x) = x^k$ with $k := \exp(S)/p$. We claim that $w(S) \neq \{1\}$ *and consists of the identity and some scalar multiples of pseudoreflections in S; furthermore,* $w(S)^{p^a} \neq S$. To see this, we work in $G = SL_{p^a+1}(q) = SL(V)$ and again note that the p-part of k is p^a. For any $g \in G$, we see that g^k is non-trivial precisely when the p-part of g is conjugate (over $\overline{\mathbb{F}}_q$) to

$$\mathrm{diag}(\lambda, \lambda^q, \ldots, \lambda^{q^{p^a-1}}, \lambda^{\frac{q^{p^a}-1}{1-q}}),$$

where $\lambda \in \mathbb{F}_{q^{p^a}}^\times$ has order p^{a+1}. Hence, g^k is either 1 or a pseudoreflection up to scalar. Now if $h = g_1 g_2 \ldots g_{p^a}$ and $g_i \in w(G)$, then we have that codim $\mathrm{Ker}(g_i - \lambda_i \cdot 1_V) \leq 1$ for some $\lambda_i \in \mathbb{F}_q^\times$. It follows that codim $\mathrm{Ker}(h - \mu \cdot 1_V) \leq p^a$, i.e. $\mathrm{Ker}(h - \mu \cdot 1_V) \neq 0$ for $\mu := \prod_{i=1}^{p^a} \lambda_i \in \mathbb{F}_q^\times$. Hence $w(S)^{p^a} \neq S$.

Kassabov and Nikolov [KN] gave more complicated examples with words that were not powers (including an example for alternating groups).

We next show that there are no such examples for alternating groups using powers.

Lemma 3.4. *Let $S = \mathsf{A}_n$ with $n \geq 5$, $\ell > 1$ an integer, and let X be the subset of S consisting of all elements whose non-trivial orbits all have size ℓ.*

(i) *If* $\ell = 2$, $X^3 = S$.
(ii) *If* ℓ *is odd,* $X^4 = S$.

Proof. The first statement follows trivially from the elementary fact that every element of the symmetric group is a product of two involutions.

Now assume that ℓ is odd. We will show that X^2 contains either an n-cycle or $(n-1)$-cycle (depending upon whether n is odd or even). We may assume that n is odd (replacing n by $n-1$ if necessary). Write $n = k\ell + r$ where $0 \le r < \ell$.

We actually prove a slightly stronger statement by induction on n (assuming n is odd). An n-cycle can be written as a product of two elements of X one of which fixes a point (and so any specified point). If $n = 5$, this is clear and more generally if $n = \ell$, this is clear.

Let $x = (1, 2, \dots, n)$ and let $y = (n, n-1, \dots, n-\ell+1)$. Note that $xy = (1, 2, \dots, n-\ell+1)$. By induction, $xy = uv$ is a product of two elements of $X \cap H$ where H is the subgroup of S fixing $\{n-\ell+2, \dots, n\}$ and moreover, we may assume that v fixes $n-\ell+1$. Thus, $x = u(vy^{-1}) \in X^2$ and u fixes a point (indeed at least $\ell - 1$ points). Applying this argument to get such an expression $x^{-1} = u_1 v_1$, we see that $x = v_1^{-1} u_1^{-1}$ with $u_1, v_1 \in X$ and u_1^{-1} fixing a point.

It follows by [B] that $X^4 = S$. □

We can now show there is a small universal bound for products of powers covering in alternating groups (as long as not every power is trivial).

Theorem 3.5. *Let* k *be a positive integer and let* $S = \mathsf{A}_n, n \ge 5$. *Assume that* k *is not a multiple of the exponent* e *of* S. *Then every element of* S *is a product of* 8 k^{th} *powers.*

Proof. Let p be a prime dividing $e/\gcd(e,k)$ and let p^{a+1} be the largest power of p dividing e. Write $n = sp^{a+1} + r$ with $0 \le r < p^{a+1}$. Then any element which is a product of sp^a disjoint p-cycles is a k^{th} power. Let Y be the set of such elements. It is straightforward to see that Y^2 contains the set of all elements of S in which all non-trivial orbits have size p. It follows by the previous result that $Y^8 = S$ (if $p = 2$, $Y^6 = S$). □

Note that if $n = 2^{a+1} - 1, a \ge 2$ and $k = e/2$ where e is the exponent of A_n, then non-trivial k^{th} powers are just the involutions moving exactly 2^a points. One sees that an n-cycle is not the product of 3 k^{th} powers.

We can show that there is a universal bound for the finite simple groups of Lie type as well under a slightly stronger hypothesis. We sketch the proof. The constant in the next results is most likely at most 5.

We point out two easy observations that we use below. In these two statements, by a finite quasisimple group of Lie type we mean any quotient of the group $\mathcal{G}^F$ in Theorem 1.1 by a central subgroup.

Corollary 3.6. *Let G be a finite quasisimple group of Lie type and let G_{rss} be the set of regular semisimple elements in G. Then $G = (G_{\mathrm{rss}})^2$.*

Proof. This is a trivial consequence of [GM] as well as Theorem 1.1, which show that any non-central element of G is contained in $(G_{\mathrm{rss}})^2$. On the other hand, if $z \in Z(G)$ and $s \in G_{\mathrm{rss}}$, then $s^{-1}z \in G_{\mathrm{rss}}$ and so $z = s \cdot s^{-1}z \in (G_{\mathrm{rss}})^2$. □

Corollary 3.7. *Let G be a finite quasisimple group of Lie type and let C be a conjugacy class of regular semisimple elements in G. Then $C^4 = G$.*

Proof. As we have already noted, it follows by [Gow] that C^2 contains all non-central semisimple elements. In particular, in the notation of Theorem 1.1 we have that

$$C^4 = C^2 \cdot C^2 \supseteq x^G \cdot y^G \supseteq G \setminus Z(G).$$

Suppose now that $z \in Z(G)$. If $s \in G$ is regular semisimple then so is $s^{-1}z$, whence $s, s^{-1}z \in C^2$ and $z = s \cdot s^{-1}z \in C^4$ as well. □

Theorem 3.8. *Let S be a finite simple group and let p be a prime dividing $|S|$. If X denotes the set of p-elements of S, then $X^{70} = S$.*

Proof. If S is sporadic, this is easily seen from the character tables. If S is an alternating group, it follows that $X^4 = S$ by Lemma 3.4. If S is a finite group of Lie type of rank at most 8, this follows by [LL].

So it suffices to prove the result for classical groups (of sufficiently large rank). We give the proof for the case $S = PSL_d(q)$ (with a better constant) and leave the other cases to the reader.

If p divides q, then $X^2 = S$ by [EG, Corollary, p. 3661]. So assume that p does not divide q. Let P be a Sylow p-subgroup of G. If $d \leq 3$, then P contains a regular semisimple element of S and so X^2 contains all semisimple elements, whence $X^4 = S$. So assume that $d \geq 4$. If $p \leq d+1$, then by the proof of Lemma 3.4, X^2 will contain either a $d+1$ cycle or d-cycle of $H := \mathsf{A}_{d+1} < S$. If $d+1$ is odd and p does not divide $d+1$, then an $(n+1)$-cycle in H is a regular semisimple element of S, whence $X^4 = S$. If $d+1$ is odd and p divides $d+1$, then similarly, we see that X^2 contains a $(d-1)$-cycle which is semisimple and has all eigenvalues of multiplicity 1 aside from 1 which has multiplicity 2. It follows that X^4 contains a regular semisimple element and so $X^{16} = S$. The same argument shows that $X^{16} = S$ for d even as well.

So assume that $p > d+1$. Let V be the natural module for $SL_d(q)$ and lift P. It is a straightforward exercise to show that P contains an element with distinct eigenvalues on $W := [P, V]$ and that $\dim W > (1/2)\dim V$. Thus, X^2 contains all semisimple elements of $\mathrm{SL}(W)$ and so X^3 contains a regular semisimple element. Thus, $X^{12} = S$. □

A restatement of the previous result in terms of powers is:

Corollary 3.9. *Let S be a finite simple group, and let d be a positive integer such that some prime p divides $|S|$ but not d. Then every element of S is a product of at most 70 d^{th} powers.*

In fact, the same proof gives:

Corollary 3.10. *Let S be a finite simple group of Lie type. Let p be a prime which is not the characteristic of S and does not divide the order of a quasi-split torus. If d is a positive integer and p divides $\exp(S)/d$, then every element of S is a product of at most 70 d^{th} powers.*

Proof. We assume that p is not the characteristic. If the rank of S is at most 8, the result follows by [LL]. So we may assume that S is classical. We give the proof for $PSL_d(q)$. First suppose that $p \le d+1$. Since p does not divide $q-1$, it follows that x^d does not vanish on $\mathsf{A}_{d+1} < S$ and we argue as above.

So assume that $p > d+1$. Then a Sylow p-subgroup P of S is abelian. Let V denote the natural module for S. So $[P,V] = W_1 \oplus \ldots \oplus W_m$ where P acts irreducibly on each W_i. Since $p > \dim W_i$, it follows that any element of P that acts non-trivially on W_i also acts irreducibly on W_i. By hypotheses, every element of $H := \Omega_1(P)$ is a d^{th} power. Now choose $1 \ne x_i \in H, 1 \le i \le m$ so that the x_i have distinct eigenvalues (over the algebraic closure). This is possible since all p^{th}-roots of 1 occur as eigenvalues and $m \dim W_1 < p$. Letting X be the image of the word x^d, it follows that X contains all semisimple elements acting on $[P,V]$. Since $\dim[P,V] > (1/2)\dim V$, it follows that X^3 contains a regular semisimple element of S and so $X^{12} = S$. ☐

Proof of Corollary 1.5. If $|S| \ge m^{8m^2}$ then we are done by Theorem 1.4. By Theorem 3.5 we are also done if $S \cong \mathsf{A}_n$. The statement is obvious if S is abelian. So we may assume that $|S| < m^{8m^2}$ and $S \not\cong \mathsf{A}_n$ (and S is non-abelian). By the assumption, there is some $1 \ne x \in S$ such that x (and so x^{-1} as well) is a m^{th} power in S. Suppose first that S is a sporadic simple group. As shown in [Z], the *covering number* $\mathrm{cn}(S)$ is at most 6, and so each element $g \in S$ is a product of at most 6 conjugates of x. Next assume that S is a simple group of Lie type, of untwisted Lie rank r. Then

$$2^{r^2} < |S| < m^{8m^2}$$

and so $r < m\sqrt{8\log_2 m}$. Now, according to the main result of [LL], every $g \in G$ is a product of at most

$$40r + 56 < 40m\sqrt{8\log_2 m} + 56 = f(m)$$

conjugates of x or x^{-1}, and so we are done.

4. Proof of Theorem 1.6

Now we proceed to prove Theorem 1.6. It suffices to prove statement (ii) of the Theorem. By choosing $N = N_{w_1,w_2}$ large enough, we may ignore all quasisimple groups G with $G/Z(G)$ being a sporadic simple group. Next, the case $G/Z(G) \cong \mathsf{A}_n$ is already settled by [LST2, Theorem 3.1]. Hence we may assume that $S := G/Z(G)$ is a finite simple group of Lie type. Again by choosing N large enough, we can ignore the cases where S has an exceptional Schur multiplier. Thus we may assume that $G = \mathcal{G}^F$ for a simple simply connected algebraic group in characteristic p and a Frobenius endomorphism $F : \mathcal{G} \to \mathcal{G}$. Furthermore, the proof of [LS, Theorem 1.7] together with [LST1, Proposition 6.4.1] establish the statement (ii) in the case $\mathcal{G}$ has bounded rank. It remains to deal with the case where $\mathcal{G}$ has unbounded rank; in particular, $\mathcal{G}$ is a classical group. Now the case $G = Spin_{2n+1}(q)$ follows from [LST2, Theorem 3.8]. Furthermore, the cases where $G \in \{SL_n(q), SU_n(q)\}$, respectively $G = Sp_{2n}(q)$, or $Spin^{\pm}_{2n}(q)$ with q even, follow from Propositions 6.2.4, 6.1.1, and 6.3.7 of [LST1].

To deal with the remaining case $G = Spin^{\pm}_{2n}(q)$ with q odd, we first recall some basic facts from spinor theory, cf. [Ch]. Let $V = \mathbb{F}_q^{2n}$ be endowed with a non-degenerate quadratic form Q. The *Clifford algebra* $\mathcal{C}(V)$ is the quotient of the tensor algebra $T(V)$ by the ideal $I(V)$ generated by $v \otimes v - Q(v)$, $v \in V$ (here we adopt the convention that $Q(v) = (v, v)$ if $(\cdot, \cdot)$ is the corresponding bilinear form on V). The natural grading on $T(V)$ passes over to $\mathcal{C}(V)$ and allows us to write $\mathcal{C}(V)$ as the direct sum of its even part $\mathcal{C}^+(V)$ and odd part $\mathcal{C}^-(V)$. We denote the identity element of $\mathcal{C}(V)$ by e. The algebra $\mathcal{C}(V)$ admits a canonical anti-automorphism α, which is defined via

$$\alpha(v_1 v_2 \dots v_r) = v_r v_{r-1} \dots v_1$$

for $v_i \in V$. The *Clifford group* $\Gamma(V)$ is the group of all invertible $s \in \mathcal{C}(V)$ such that $sVs^{-1} \subseteq V$. The action of $s \in \Gamma(V)$ on V defines a surjective homomorphism $\phi : \Gamma(V) \to GO(V)$ with $\mathrm{Ker}(\phi) = \mathbb{F}_q^{\times} e$. If $v \in V$ is nonsingular, then $-\phi(v) = \rho_v$, the reflection corresponding to v. The *special Clifford group* $\Gamma^+(V)$ is $\Gamma(V) \cap \mathcal{C}^+(V)$. Let $\Gamma_0(V) := \{s \in \Gamma(V) \mid \alpha(s)s = e\}$. The *reduced Clifford group*, or the *spin group*, is $Spin(V) = \Gamma^+(V) \cap \Gamma_0(V)$. The sequences

$$1 \longrightarrow \mathbb{F}_q^{\times} e \longrightarrow \Gamma^+(V) \xrightarrow{\phi} SO(V) \longrightarrow 1,$$

$$1 \longrightarrow \langle -e \rangle \longrightarrow Spin(V) \xrightarrow{\phi} \Omega(V) \longrightarrow 1$$

are exact.

If A is a non-degenerate subspace of V, then we denote by C_A the subalgebra of $\mathcal{C}(V)$ generated by all $a \in A$. We now clarify the relationship between C_A and the

Clifford algebra $\mathcal{C}(A)$ of the quadratic space $(A, Q|_A)$. Decompose $V = A \oplus A^\perp$. We will need the following statement:

Lemma 4.1. *Let (V, Q) be a non-degenerate quadratic space over a field $\mathbb{F}_q$ of odd characteristic. Suppose A is a non-degenerate subspace of dimension ≥ 2 of V, and let C_A be the subalgebra of $\mathcal{C}(V)$ generated by all $a \in A$. Then there is a (canonical) algebra isomorphism $\psi : \mathcal{C}(A) \cong C_A$ which induces a group isomorphism $Spin(A) \cong C_A \cap Spin(V)$. Furthermore, if $g \in Spin(V)$ is such that $\phi(g)$ acts trivially on $A^\perp$, then $g \in C_A \cap Spin(V)$. Finally, if $h \in C_A \cap Spin(V)$ is such that $\psi^{-1}(h)$ projects onto -1_A then $\phi(h) = \mathrm{diag}(-1_A, 1_{A^\perp})$.*

Proof. The first statement is just [LBST2, Lemma 4.1]. For the second statement, it was shown by the same lemma that ϕ projects $C_A \cap Spin(V)$ onto the subgroup

$$X := \{x \in \Omega(V) \mid x|_{A^\perp} = 1_{A^\perp}\}$$

with kernel $\langle -e \rangle$. By the assumption, $\phi(g)$ belongs to X. Hence, there are exactly two elements g' and $-eg'$ in $C_A \cap Spin(V)$ such that $\phi(g') = \phi(-eg') = \phi(g)$. Recall that ϕ also projects G onto $\Omega(V)$ with kernel $\langle -e \rangle$. It follows that $g \in \{g', -eg'\}$, and so $g \in C_A \cap Spin(V)$.

For the third statement, observe that the isomorphism ψ sends $a + I(A)$ (which is identified with a in $\mathcal{C}(A)$) to $a + I(V)$ (which is identified with a in $\mathcal{C}(V)$) for any $a \in A$. By assumption, $h' := \psi^{-1}(h)$ projects onto -1_A (under the natural map $\Gamma(A) \to GO(A)$). Hence $h'ah'^{-1} = -a$ for all $a \in A$. Applying ψ^{-1}, we obtain $hah^{-1} = -a$ for all $a \in A$, yielding $\phi(h)|_A = -1_A$. On the other hand, $\phi(h)|_{A^\perp} = 1_{A^\perp}$ as $h \in C_A \cap Spin(V)$ and ϕ maps $C_A \cap Spin(V)$ onto X. $\square$

Using Theorem 2.7 we can prove the following key extension of [LST1, Proposition 6.3.6]:

Proposition 4.2. *Let w_1 and w_2 be non-trivial words and let $k, l \geq 3$ be two coprime odd integers. Fix an integer $v > 0$ such that $l|(kv-1)$. Then there exists an integer L such that for all $n = k(2al + v)$ with $a \geq L$, $\epsilon = \pm$, and for all q,*

$$w_1(Spin^\epsilon_{2n}(q))w_2(Spin^\epsilon_{2n}(q)) \supseteq Spin^\epsilon_{2n}(q) \setminus Z(Spin^\epsilon_{2n}(q)).$$

Proof. Note that the case $\epsilon = -$ and the case where $\epsilon = +$ but v is odd are already covered by [LST1, Proposition 6.3.6]. So we may assume that $\epsilon = +$ and $2|v$. Observe that $l|(n-1)$ for any $n = k(2al + v)$. As in the proof of [LST1, Proposition 6.3.6], there exists L depending on k, l, w_1, and w_2, such that for all $n = k(2al + v)$ with $a > L$, $w_1(Spin^+_{2l}(q^{(n-1)/l}))$ contains a regular semisimple element x_1 of type T^+_{n-1} in

$$i^+(Spin^+_{2l}(q^{(n-1)/l})) < Spin^+_{2n-2}(q),$$

and $w_2(Spin^-_{2l}(q^{(n-1)/l}))$ contains a regular semisimple element x_2 of type T^-_{n-1} in

$$i^-(Spin^-_{2l}(q^{(n-1)/l})) < Spin^-_{2n-2}(q).$$

(Here $i^{\pm}$ are natural embeddings by base change.) Note that, under the natural embedding $Spin^+_{2n-2}(q) \hookrightarrow G := Spin^+_{2n}(q)$, x_1 becomes a regular semisimple element of type $T^{+,+}_{n-1,1}$ of $Spin^+_{2n}(q)$. Similarly, under the natural embedding $Spin^-_{2n-2}(q) \hookrightarrow G$, x_2 becomes a regular semisimple element of type $T^{-,-}_{n-1,1}$ of $Spin^+_{2n}(q)$. By Theorem 2.7, $x_1^G \cdot x_2^G \supseteq G \setminus Z(G)$, and so we are done. □

Now Theorem 1.6 follows from

Theorem 4.3. *Let $w = w_1w_2$, where w_1 and w_2 are non-trivial disjoint words. Then there is an integer $D = D_{w_1,w_2}$ such that for all $G = Spin^{\epsilon}_{2n}(q)$ with $n > D$, q odd, and $\epsilon = \pm$, we have $w(G) \supseteq G \setminus Z(G)$.*

Proof. 1) Let $V = \mathbb{F}_q^{2n}$ be a quadratic space with quadratic form Q corresponding to $G \cong Spin(V)$, and consider the canonical projection $\phi : G \to \Omega(V)$. We will also denote the central element $-e$ of $Spin(V)$ by z. For any $g \in G$, by the *support* $\mathrm{supp}(g)$ *of* g we mean the support $\mathrm{supp}(\phi(g))$ of the element $\phi(g) \in \Omega(V)$.

We will follow in parts the proof of [LST1, Proposition 6.3.7]. As shown in part 1) of the proof of [LST1, Proposition 6.3.5], if n is sufficiently large then $w_1(G)$ and $w_2(G)$ contains regular semisimple elements t_1 and t_2 of type $T^{+,\epsilon}_{a,n-a}$ and $T^{-,-\epsilon}_{a+1,n-a-1}$, respectively, with a odd and bounded. Arguing as in part 2) of the proof of [LST1, Proposition 6.3.5] and using Proposition 3.3.1 and Theorem 1.2.1 of [LST1], we can reduce to the case of elements g of bounded support $\leq B$ (where B depends on w_1, w_2). Thus it suffices to prove that if $g \in G \setminus Z(G)$ is of bounded support $\leq B$ and n is sufficiently large, then $g \in w(G)$.

2) Assuming $n \geq B+2$, we see that $\phi(g)$ has a (unique) primary eigenvalue $\lambda = \pm 1$. By [LST1, Lemma 6.3.4], g fixes an orthogonal decomposition $V = U \oplus W$, where $\phi(g)|_U = \lambda \cdot 1_U$, and $\dim U \geq 2n - 2B \geq 4$. Suppose $\lambda = 1$. Then we can write $V = A \oplus A^{\perp}$, where $A^{\perp}$ is a 1-dimensional non-degenerate subspace of U. By Lemma 4.1, $g \in X := C_A \cap Spin(V)$ and $X \cong Spin(A) = Spin_{2n-1}(q)$. By [LST2, Theorem 3.8], $g \in w(X) \subseteq w(G)$ if n is large enough.

3) It remains to consider the case $\lambda = -1$. By [LST1, Proposition 6.3.2], there exists an even M (depending on w_1, w_2) such that, for any $b \geq 1$, $w(Spin^+_{2bM}(q))$ contains an element which projects onto $-I$ (negative the identity transformation on $\mathbb{F}_q^{2bM}$). Fix coprime odd integers $k, l \geq 3$ which are coprime to $2M$. Also, fix an integer $v > 0$ such that $l|(kv-1)$ and $2|(n-v)$. Then by Proposition 4.2, there exists $L \geq B$ (depending on w_1, w_2) such that

$$w(Spin^{\gamma}_{2m}(q)) \supseteq Spin^{\gamma}_{2m}(q) \setminus Z(Spin^{\gamma}_{2m}(q))$$

for all $m = k(2al + v)$ with $a \geq L$ and all $\gamma = \pm$.

Now assume that $n > kl(2L + M) + kv$. Arguing as in the proof of [LST1, Proposition 6.3.7], we see that g preserves the orthogonal decomposition $V = \tilde{V} \oplus \tilde{U}$, where $\dim \tilde{V} = 2yM$ for some integer $y \geq 1$, $\tilde{V}$ is of type $+$, $\phi(g)|_{\tilde{V}} = -1_{\tilde{V}}$,

$\dim \tilde{U} = k(2xl + v)$ for some integer $x > L$, and g has at least two eigenvalues -1 on $\tilde{U}$. As mentioned above, by [LST1, Proposition 6.3.2], there is some element $h' \in w(Spin(\tilde{V}))$ that lies above $-1_{\tilde{V}}$. By Lemma 4.1, there is a group isomorphism

$$\psi \ : \ Y_1 := C_{\tilde{V}} \cap G \cong Spin(\tilde{V}),$$

and furthermore, $h := \psi^{-1}(h')$ belongs to $w(Y_1)$ and satisfies

$$\phi(h) = \mathrm{diag}(1_{\tilde{U}}, -1_{\tilde{V}}).$$

Now gh^{-1} fixes the decomposition $V = \tilde{V} \oplus \tilde{U}$ and acts trivially on $\tilde{V}$. By Lemma 4.1,

$$gh^{-1} \in Y_2 := C_{\tilde{U}} \cap G \cong Spin(\tilde{U}).$$

Clearly, gh^{-1} and g have the same action on $\tilde{U}$ and so they both have at least two eigenvalues -1 on $\tilde{U}$ by the construction of $\tilde{U}$ and $\tilde{V}$. If $\phi(gh^{-1})|_{\tilde{U}} = -1_{\tilde{U}}$, then $\phi(g) = -1_V$ and so $g \in Z(G)$, contrary to the choice of g. So we may assume that $\phi(gh^{-1})|_{\tilde{U}}$ is not scalar. Thus $gh^{-1} \in Y_2 \setminus Z(Y_2)$. Since $x > L$, by Proposition 4.2 applied to $Y_2 \cong Spin(\tilde{U})$ we have $gh^{-1} \in w(Y_2)$. Finally, since Y_1 and Y_2 commute by [TZ2, Lemma 6.1], we conclude that

$$g = gh^{-1} \cdot h \in w(Y_2)w(Y_1) \subseteq w(G),$$

as stated. □

References

[B] E. Bertram, Even permutations as a product of two conjugate cycles, *J. Comb. Theory Ser. A* **12** (1972), 368–380.

[C] R. Carter, '*Finite Groups of Lie type: Conjugacy Classes and Complex Characters*', Wiley, Chichester, 1985.

[Ch] C. Chevalley, *The Algebraic Theory of Spinors and Clifford Algebras. Collected works*, vol. **2**, Springer-Verlag, Berlin, 1997.

[Atlas] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, '*An ATLAS of Finite Groups*', Clarendon Press, Oxford, 1985.

[DL] P. Deligne and G. Lusztig, Representations of reductive groups over finite fields, *Annals of Math.* **103** (1976), 103–161.

[Der] D. I. Deriziotis, '*Conjugacy Classes and Centralizers of Semisimple Elements in Finite Groups of Lie Type*', Vorlesungen aus dem Fachbereich Mathematik der Universität Essen, Heft 11, 1984.

[DM] F. Digne and J. Michel, '*Representations of Finite Groups of Lie Type*', London Mathematical Society Student Texts **21**, Cambridge University Press, 1991.

[Do] L. Dornhoff, '*Group Representation Theory*', Marcel Dekker, New York, 1972.

[EG] E. W. Ellers and N. Gordeev, On the conjectures of J. Thompson and O. Ore, *Trans. Amer. Math. Soc.* **350** (1998), 3657–3671.

[FST] J. Fulman, J. Saxl, and Pham Huu Tiep, Cycle indices for finite orthogonal groups of even characteristic, *Trans. Amer. Math. Soc.* **364** (2012), 2539–2566.

[GAP] The GAP group, '`GAP` - *groups, algorithms, and programming*', Version 4.4, 2004, `http://www.gap-system.org`.

[Chev] M. Geck, G. Hiss, F. Lübeck, G. Malle, G. Pfeiffer, CHEVIE – A system for computing and processing generic character tables for finite groups of Lie type, Weyl groups and Hecke algebras. Appl. Algebra Engrg. Comm. Comput. **7** (1996), 175–210.

[Gow] R. Gow, Commutators in finite simple groups of Lie type, *Bull. London Math. Soc.* **32** (2000), 311–315.

[GM] R. M. Guralnick and G. Malle, Product of conjugacy classes and fixed point spaces, *J. Amer. Math. Soc.* **25** (2012), 77–121.

[GMT] R. M. Guralnick, G. Malle, and Pham Huu Tiep, Product of conjugacy classes in finite simple classical groups, (in preparation).

[GT] R. M. Guralnick and Pham Huu Tiep, Lifting in Frattini covers and a characterization of finite solvable groups, (submitted).

[HSTZ] G. Heide, J. Saxl, Pham Huu Tiep, and A. E. Zalesski, Conjugation action, induced representations, and the Steinberg square for simple groups of Lie type, *Proc. London Math. Soc.* (to appear).

[KN] M. Kassabov and N. Nikolov, Words with few values in finite simple groups, *Quarterly J. Math.* (to appear).

[LMT] M. Larsen, G. Malle, and Pham Huu Tiep, The largest irreducible representations of simple groups, *Proc. London Math. Soc.* (to appear).

[LS] M. Larsen and A. Shalev, Word maps and Waring type problems, *J. Amer. Math. Soc.* **22** (2009), 437–466.

[LST1] M. Larsen, A. Shalev, and Pham Huu Tiep, Waring problem for finite simple groups, *Annals of Math.* **174** (2011), 1885–1950.

[LST2] M. Larsen, A. Shalev, and Pham Huu Tiep, Waring problem for finite quasisimple groups, *Int. Math. Res. Notices* (to appear).

[LL] R. Lawther and M. W. Liebeck, On the diameter of a Cayley graph of a simple group of Lie type based on a conjugacy class, *J. Combin. Theory Ser. A* **83** (1998), 118–137.

[LBST1] M. W. Liebeck, E. O'Brien, A. Shalev, and Pham Huu Tiep, The Ore conjecture, *J. Europ. Math. Soc.* **12** (2010), 939–1008.

[LBST2] M. W. Liebeck, E. O'Brien, A. Shalev, and Pham Huu Tiep, Commutators in finite quasisimple groups, *Bull. London Math. Soc.* **43** (2011), 1079–1092.

[Lu] F. Lübeck, Character degrees and their multiplicities for some groups of Lie type of rank < 9, http://www.math.rwth-aachen.de/∼Frank.Luebeck/chev/DegMult/index.html

[LuM] F. Lübeck and G. Malle, $(2,3)$-generation of exceptional groups, *J. London Math. Soc.* **59** (1999), 109–122.

[MSW] G. Malle, J. Saxl, and T. Weigel, Generation of classical groups, *Geom. Dedicata* **49** (1994), 85–116.

[M1] G. Malle, Die unipotenten Charaktere von ${}^2F_4(q^2)$, *Comm. Algebra* **18** (1990), 2361–2381.

[M2] G. Malle, Unipotente Grade imprimitiver komplexer Spiegelungsgruppen. *J. Algebra* **177** (1995), 768–826.

[MZ] C. Martinez and E. Zelmanov, Products of powers in finite simple groups, *Israel J. Math.* **96** (1996), 469–479.

[MT] A. Moretó and Pham Huu Tiep, Prime divisors of character degrees, *J. Group Theory* **11** (2008), 341–356.

[N] Hung Ngoc Nguyen, Low-dimensional characters of the symplectic and orthogonal groups, *Comm. Algebra* **38** (2010), 1157–1197.

[NS] N. Nikolov and D. Segal, Powers in finite groups, *Groups Geom. Dyn.* **5** (2011), 501–507.

[R] P. Ribenboim, '*The Book of Prime Number Records*', Springer-Verlag, N. Y. at al, 1988.

[SW] J. Saxl and J. S. Wilson, A note on powers in simple groups, *Math. Proc. Cambridge Philos. Soc.*, **122** (1997), 91–94.

[Sh] A. Shalev, Word maps, conjugacy classes, and a noncommutative Waring-type theorem, *Ann. of Math.* **170** (2009), 1383–1416.

[ST] P. Sin and Pham Huu Tiep, Rank 3 permutation modules for finite classical groups, *J. Algebra* **291** (2005), 551–606.

[Sri] B. Srinivasan, The characters of the finite symplectic group $Sp(4, q)$, *Trans. Amer. Math. Soc.* **131** (1968), 488–525.

[TZ1] Pham Huu Tiep and A.E. Zalesskii, Minimal characters of the finite classical groups, *Comm. Algebra* **24** (1996), 2093–2167.

[TZ2] Pham Huu Tiep and A. E. Zalesskii, Real conjugacy classes in algebraic groups and finite groups of Lie type, *J. Group Theory* **8** (2005), 291–315.

[Z] I. Zisser, Covering number of the sporadic simple groups, *Israel J. Math.* **67** (1989), 217–224.

[Zs] K. Zsigmondy, Zur Theorie der Potenzreste, *Monath. Math. Phys.* **3** (1892), 265–284.

Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, USA

E-mail address: `guralnic@usc.edu`

Department of Mathematics, University of Arizona, Tucson, AZ 85721-0089, USA

E-mail address: `tiep@math.arizona.edu`